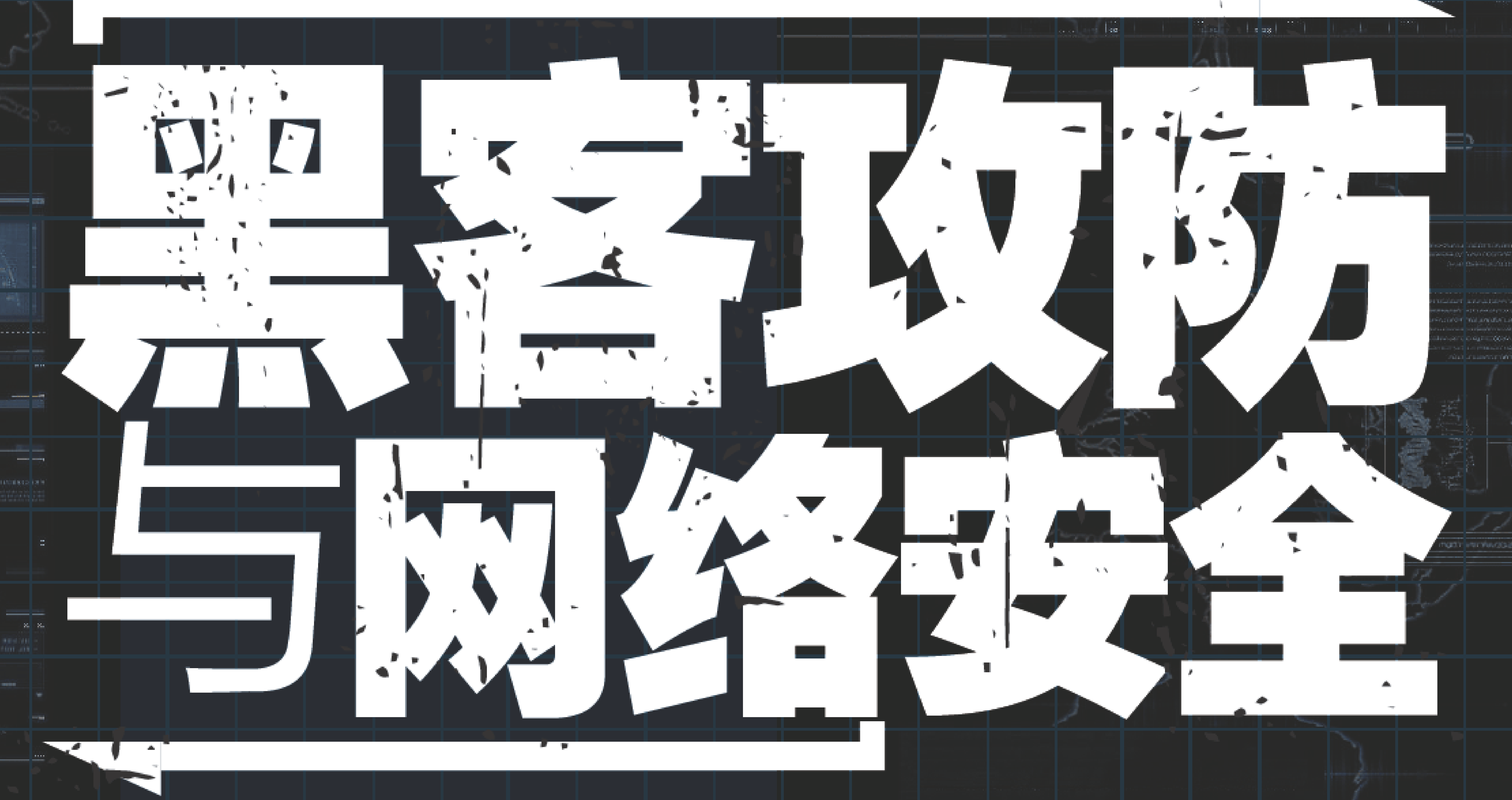
从新手到高手

黑客入门与网络安全实用手册
安全技术全新升级



黑客攻防与网络安全

从新手到高手（实战篇）



网络安全技术联盟 主 编
魏 红 副主编



一线网络安全技术联盟倾心打造
海量王牌资源超值赠送

- 超值赠送1 同步微视频
- 超值赠送2 精美教学PPT课件
- 超值赠送3 黑客工具（107个）速查手册
- 超值赠送4 常用黑客命令（160个）速查手册
- 超值赠送5 180页常见故障维修手册
- 超值赠送6 191页Windows 10系统使用和防护技巧
- 超值赠送7 8大经典密码破解工具详解
- 超值赠送8 加密与解密技术快速入门小白电子手册
- 超值赠送9 网站入侵与黑客脚本编程电子书
- 超值赠送10 黑客命令全方位详解电子书

清华大学出版社

黑客攻防与网络安全从新手到高手（实战篇）

网络安全技术联盟　主　编
魏红　副主篇

清華大学出版社
北　京

内容简介

本书在剖析用户进行黑客防御中迫切需要或想要用到的技术时，力求对其进行“傻瓜”式的讲解，使读者对网络防御技术有一个系统的了解，能够更好地防范黑客的攻击。全书共分为 15 章，包括网络安全快速入门、搭建网络安全测试环境、黑客入侵方式与 DOS 命令、木马病毒的查杀与预防、系统漏洞与用户账户的安全防护、远程控制入侵系统的安全防护、网络账号及密码的安全防护、浏览器的安全防护、有线局域网的安全防护、无线局域网的安全防护、网站系统的安全防护、电子邮箱与邮件的安全防护、操作系统的安全防护、计算机安全的终极防护、黑客后门入侵痕迹的清理等内容。

另外，本书还赠送海量王牌资源，由于赠送的资源比较多，在本书前言部分对赠送资源的具体内容做了详细说明，帮助读者掌握黑客防守方方面面的知识。

本书内容丰富，图文并茂，深入浅出，不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，还可作为大中专院校相关专业的参考书。

图书在版编目(CIP)数据

黑客攻防与网络安全从新手到高手：实战篇 / 网络安全技术联盟主编. —北京：清华大学出版社，2019
（从新手到高手）
ISBN 978-7-302-53011-4

Ⅰ.①黑… Ⅱ. ①网… Ⅲ. ①黑客—网络防御 Ⅳ. ①TP393.081

中国版本图书馆CIP数据核字（2019）第094003号

责任编辑：张　敏
封面设计：杨玉兰
责任校对：胡伟民
责任印制：丛怀宇

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn， http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　　邮　　编：100084
社 总 机：010-62770175　　　邮　　购：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：18.25　　字　　数：460千字
版　　次：2019年10月第1版　　印　　次：2019年10月第1次印刷
定　　价：69.80元

产品编号：082954-01

Preface
前　言

随着手机、平板计算机的普及，无线网络的防范变得尤为重要，为此，本书除了讲解有线网络的攻防策略外，还把目前市场上流行的无线攻防等热点融入其中。

本书特色

知识丰富全面：知识点由浅入深，涵盖了所有黑客攻防技术，使读者由浅入深地掌握黑客攻防方面的技能。

图文并茂：注重操作，在介绍案例的过程中，每一个操作均有对应的插图。这种图文结合的方式使读者在学习过程中能够直观、清晰地看到操作的过程以及效果，便于更快地理解和掌握。

案例丰富：把知识点融汇于系统的案例实训当中，并且结合经典案例进行讲解和拓展，进而达到“知其然，并知其所以然”的效果。

提示技巧、贴心周到：本书对读者在学习过程中可能会遇到的疑难问题以“提示”的形式进行了说明，以免读者在学习的过程中走弯路。

超值赠送

本书将赠送同步微视频、精美教学PPT课件、黑客工具（107个）速查手册、常用黑客命令（160个）速查手册、180页常见故障维修手册、191页Windows 10系统使用和防护技巧、8大经典密码破解工具详解、加密与解密技术快速入门小白电子手册、网站入侵与黑客脚本编程电子书、黑客命令全方位详解电子书。读者可扫描右方二维码或通过电子邮件zhangmin2@tup.tsinghua.edu.cn获取本书资源。



精美教学幻灯片



赠送资源8本电子书

读者对象

本书不仅适用于网络安全从业人员及网络管理员，而且适用于广大网络爱好者，还可作为大中专院校相关专业的参考书。

写作团队

本书由长期研究网络安全知识的网络安全技术联盟主编，魏红任副主编，另外还有王秀英、王英英、刘玉萍、刘尧、王朵朵、王攀登、王婷婷、张芳、李小威、王猛、王维维、李佳康、王秀荣、王天护、皮素芹等人参与编写工作。在编写过程中，尽所能地将最好的讲解呈现给读者，但也难免有疏漏和不妥之处，敬请不吝指正。若您在学习中遇到困难或疑问，或有何建议，可通过电子邮箱zhangmin2@tup.tsinghua.edu.cn及时获得在线指导和本书的资源。

编　者

Contents

目 录

第1章　网络安全快速入门

随着信息时代的发展和网络的普及，越来越多的人走进了网络生活，然而人们在享受网络带来便利的同时，也时刻面临着黑客们残酷攻击的危险。本章介绍网络安全的相关技术信息，主要内容包括网络中的相关概念、网络通信的相关协议、IP地址、MAC地址、端口、系统进程等。

1.1　网络中的相关概念

在网络安全中，经常会接触到很多和网络有关的概念，如浏览器、URL、FTP、IP地址及域名等，理解这些概念，对保护网络安全有一定的帮助。

1.1.1　互联网与因特网

互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来的结果。互联网在现实生活中应用很广泛，在互联网上人们可以聊天、玩游戏、查阅资料等。互联网是全球性的，这就意味着这个网络不管是谁发明了它，是属于全人类的。

因特网是一个把分布于世界各地的计算机用传输介质互相连接起来的网络，它是基于TCP/IP实现的。TCP/IP由很多协议组成，不同类型的协议又被放在不同的层，其中，位于应用层的协议就有很多，如FTP、SMTP、HTTP。

1.1.2　万维网与浏览器

万维网（World Wide Web，WWW）简称为3W，它是无数个网络站点和网页的集合，也是因特网提供的最主要的服务。万维网是由多媒体链接而形成的集合，通常我们上网看到的内容就是万维网的内容。如下图所示为使用万维网打开的百度首页。



提示：互联网、因特网、万维网三者的关系是由互联网包含因特网，因特网包含万维网。凡是由能彼此通信的设备组成的网络就叫互联网。所以，即使仅有两台计算机，不论用何种技术使其彼此通信，也叫互联网。

浏览器是将互联网上的文本文档（或其他类型的文件）翻译成网页，并让用户与这些文件交互的一种软件工具，主要用于查看网页的内容。目前最常用的浏览器有微软公司的Internet Explorer（通常称为IE浏览器），如下图所示是使用IE浏览器打开的页面。



1.1.3 URL地址与域名

URL（Uniform Resource Locator）即统一资源定位器，也就是网络地址，是在因特网上用来描述信息资源，并将因特网提供的服务统一编址的系统。简单来说，通常在IE浏览器或Netscape浏览器中输入的网址就是URL的一种，如百度网址http://www.baidu.com。

域名（Domain Name）类似于因特网上的门牌号，是用于识别和定位互联网上计算机层次结构的字符标识，与该计算机的因特网协议（IP）地址相对应。但相对于IP地址而言，域名更便于使用者理解和记忆。URL和域名是两个不同的概念，如http://www.sohu.com/是URL，而www.sohu.com是域名，如下图所示为使用URL打开的网页。



1.1.4 IP地址与MAC地址

IP地址用于在TCP/IP中标记每台计算机的地址，通常使用十进制来表示，如192.168.1.100，但在计算机内部，IP地址是一个32位的二进制数值，如11000000 10101000 00000001 00000110（192.168.1.6）。

MAC地址与网络无关，即无论将带有这个地址的硬件（如网卡、集线器、路由器等）接入到网络的何处，都是相同的MAC地址，它由厂商写在网卡的BIOS里。

MAC地址通常表示为12位十六进制数，每2位十六进制数之间用冒号隔开，如08:00:20:0A:8C:6D就是一个MAC地址，其中前6位（08:00:20）代表网络硬件制造商的编号，它由IEEE分配，而后6位（0A:8C:6D）代表该制造商所制造的某个网络产品（如网卡）的系列号。每个网络制造商必须确保它所制造的每个以太网设备前3个字节都相同，后3个字节不同，这样，就可以保证世界上每个以太网设备都具有唯一的MAC地址。

提示：IP地址与MAC地址的区别在于IP地址基于逻辑，比较灵活，不受硬件限制，也容易记忆；MAC地址在一定程度上与硬件一致，基于物理，能够具体标识。这两种地址均有各自的长处，使用时也因条件不同而采取不同的地址。

1.2 认识网络通信协议

“网络通信协议”是计算机网络的一个重要组成部分，是不同网络之间通信、“交流”的公共语言。有了它，使用不同系统的计算机或网络之间才可以彼此识别，识别出不同的网络操作指令，建立信任关系。

1.2.1 TCP/IP

TCP/IP包括两个子协议，即TCP（Transmission Control Protocol，传输控制协议）和IP（Internet Protocol，因特网协议）。在这两个子协议中又包括许多应用型的协议和服务，使得TCP/IP的功能非常强大。

TCP/IP中除了包括TCP、IP两个协议外，还包括许多子协议。它的核心协议包括用户数据报协议（UDP）、地址解析协议（ARP）及因特网控制消息协议（ICMP）等。

1.2.2　IP

IP（Internet Protocol，因特网协议）可实现两个基本功能：寻址和分段。IP可以根据数据报报头中包括的目的地址将数据报传送到目的地址。另外，IP使用4个关键技术提供服务：服务类型、生存时间、选项和报头校验码。

IP的基本任务是通过互联网传送数据报，各个IP数据报之间是相互独立的。IP从源运输实体取得数据，通过它的数据链路层服务传给目的主机的IP层。在传送时，高层协议将数据传给IP，IP再将数据封装为互联网数据报，并交给数据链路层协议通过局域网传送。

1.2.3　ARP

ARP（Address Resolution Protocol，地址解析协议）基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。在局域网中，网络中实际传输的是“帧”，帧里面有目标主机的MAC地址。

在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址，这个MAC地址就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送数据帧前将目标IP地址转换成目标MAC地址的过程。

1.2.4　ICMP

ICMP（Internet Control Message Protocol，因特网控制消息协议）是TCP/IP中的子协议，主要用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要作用。

ICMP对于网络安全非常重要，因为ICMP本身的特点，决定了它非常容易被用来攻击网络上的路由器和主机。例如，可以利用操作系统规定的ICMP数据包最大尺寸不超过64KB这一规定，向主机发起Ping of Death（死亡之Ping）攻击。

1.3　计算机基本信息的获取

一台计算机的基本信息包括IP地址、物理地址、端口信息、系统进程信息、注册表信息等各种系统信息，用户要想提高计算机的安全系数，必须要学会查看计算机基本信息的方法。

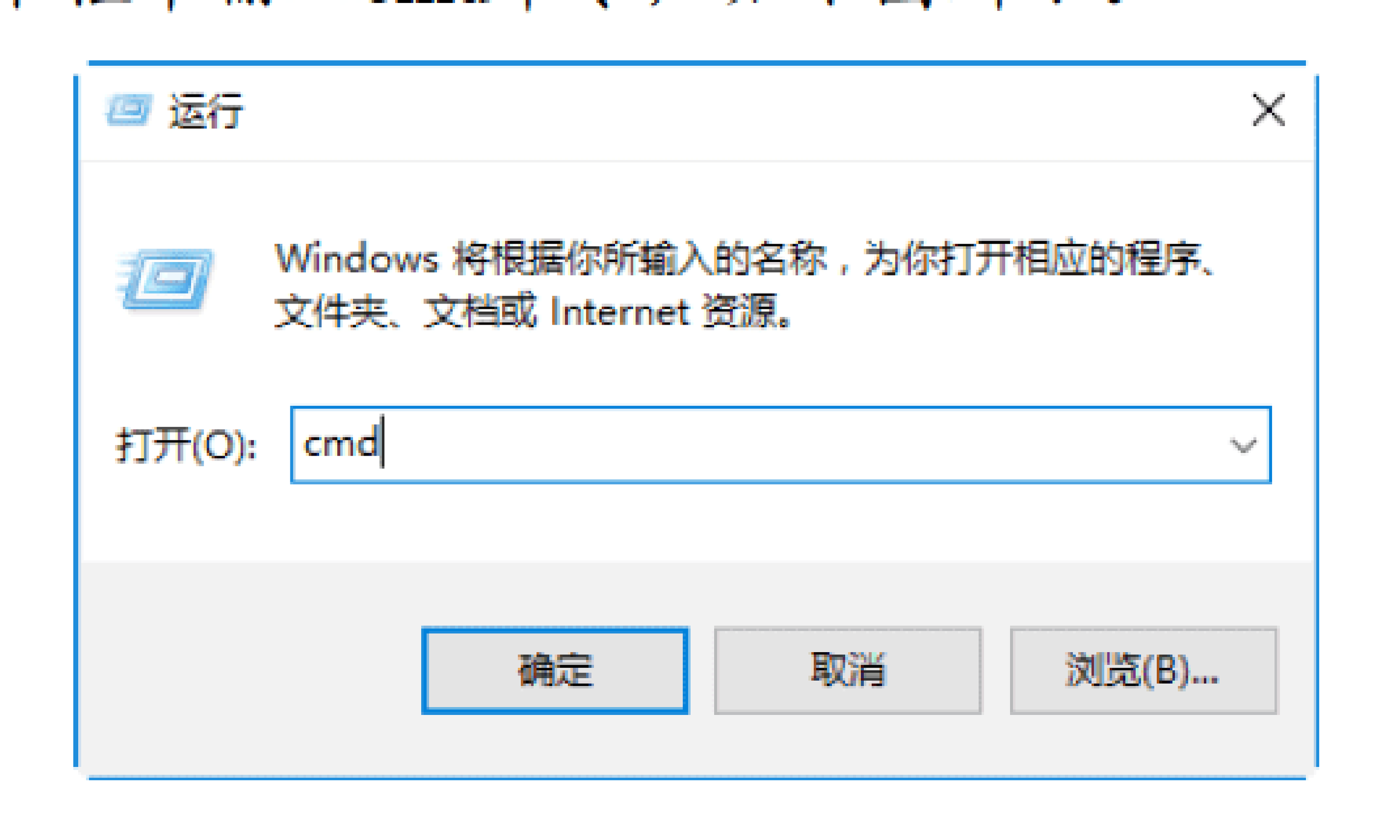
实战1：获取本机的IP地址

在互联网中，一台主机只有一个IP地址，因此，黑客要想攻击某台主机，必须找到这台主机的IP地址，然后才能进行入侵攻击，可以说IP地址是黑客实施入侵攻击的一个关键。使用ipconfig命令可以获取本地计算机的IP地址，具体的操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中执行“运行”命令，如下图所示。



Step 02 打开“运行”对话框，在“打开”文本框中输入cmd命令，如下图所示。



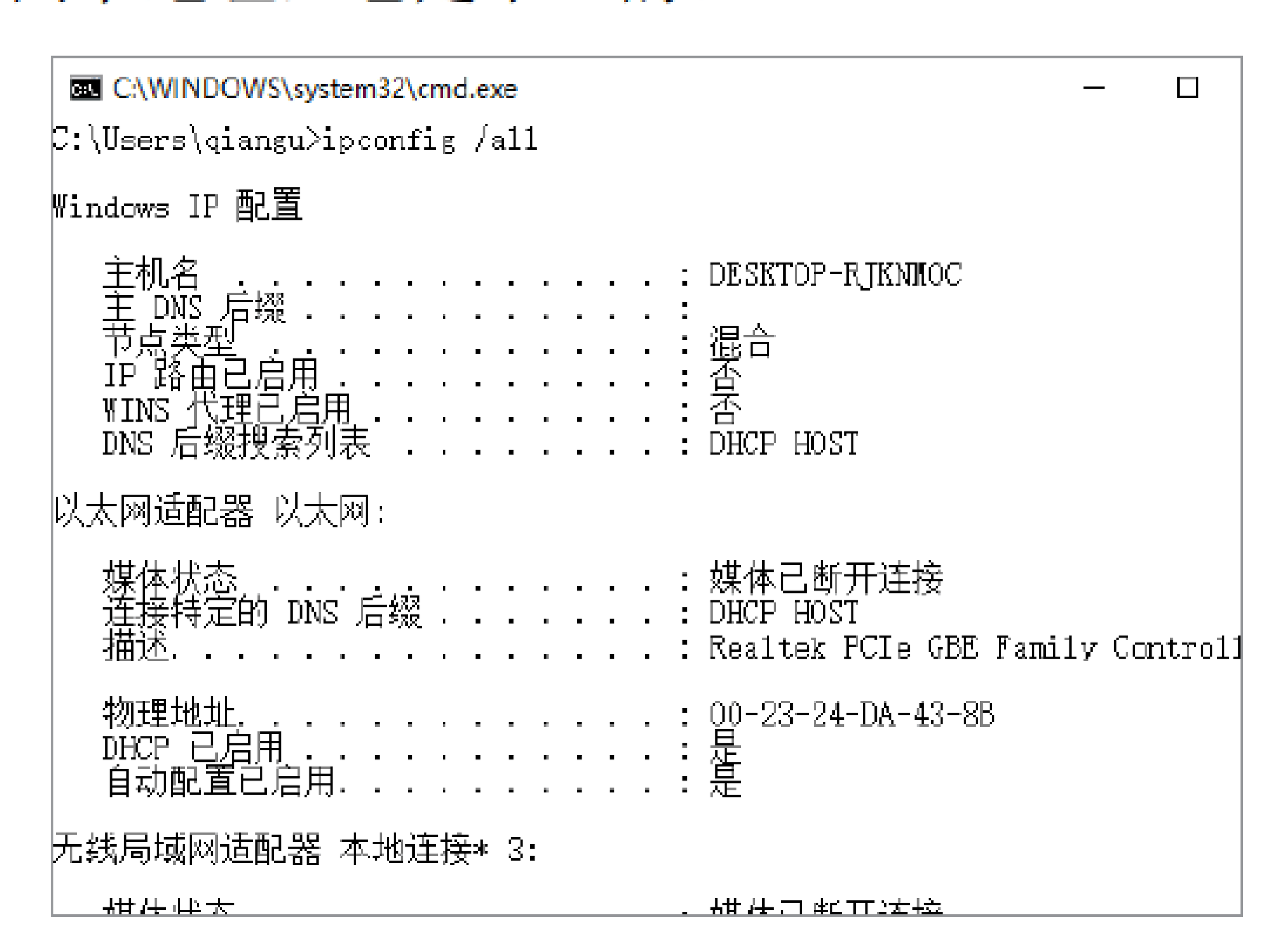
Step 03 单击“确定”按钮，打开“命令提示符”窗口，在“命令提示符”窗口中输入

ipconfig，按Enter键，即可显示出本机的IP配置相关信息。

提示：在“命令提示符”窗口中，192.168.0.130表示本机在局域网中的IP地址。

实战2：获取本机的物理地址

在“命令提示符”窗口中输入ipconfig /all命令，然后按Enter键，可以在显示的结果中看到一个物理地址：00-23-24-DA-43-8B，这就是本机的物理地址，也是本机的网卡地址，它是唯一的。

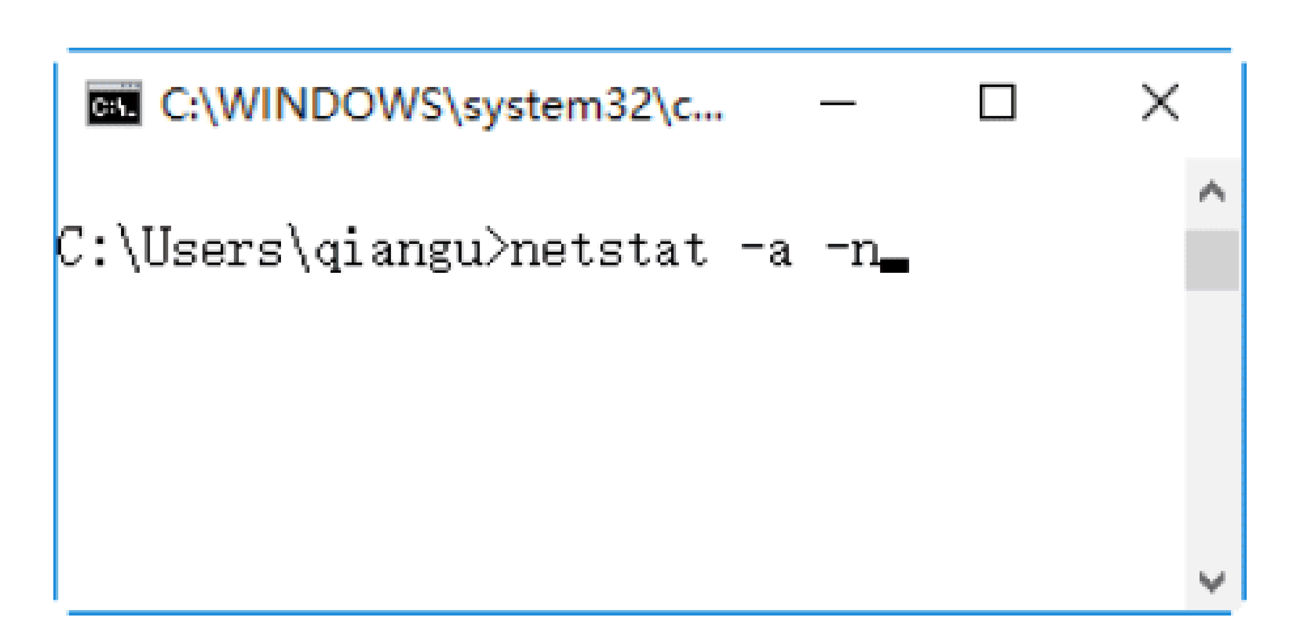




实战3：查看系统开放的端口

经常查看系统开放端口的状态变化，可以帮助计算机用户及时维护系统安全，防止黑客通过端口入侵计算机。用户可以使用netstat命令查看自己系统端口状态。具体的操作步骤如下。

Step 01 打开“命令提示符”窗口，在其中输入netstat –a –n命令，如下图所示。



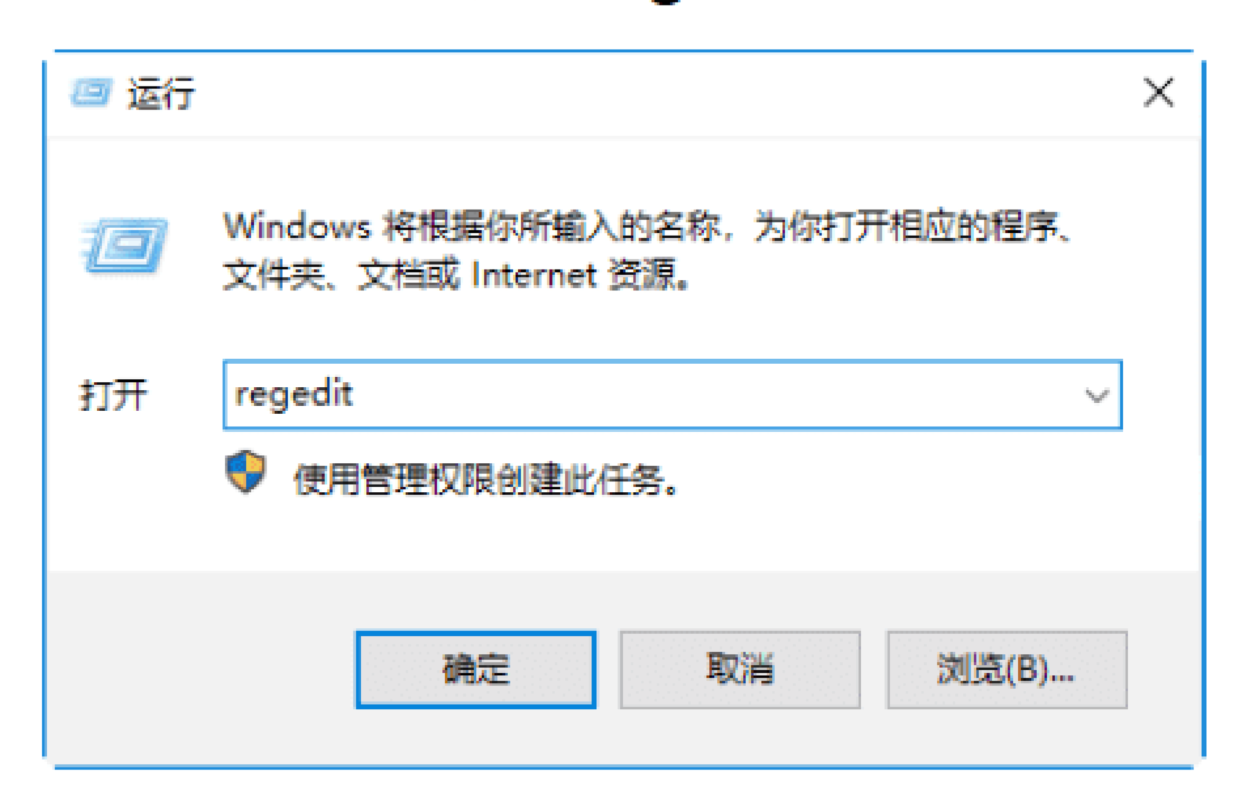
Step 02 按Enter键，即可看到以数字显示的TCP和UCP连接的端口号及其状态，如下图所示。



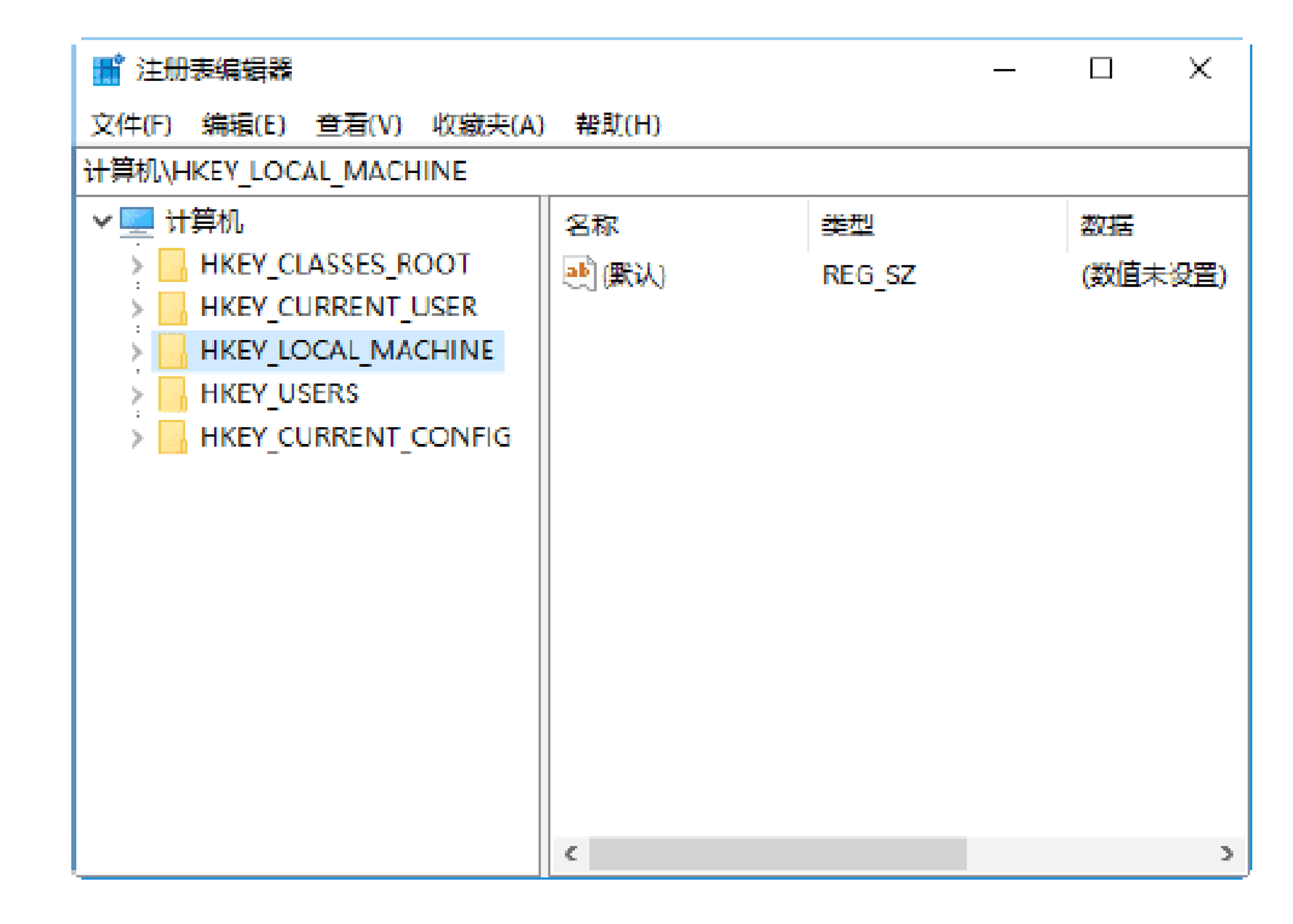
实战4：查看系统注册表信息

注册表（Registry）是Microsoft Windows中的一个重要数据库，用于存储系统和应用程序的设置信息。通过注册表，用户可以添加、删除、修改系统内的软件配置信息或硬件驱动程序。查看Windows系统中注册表信息的操作步骤如下。

Step 01 在Windows操作系统中选择“开始”→“运行”选项，打开“运行”对话框，在其中输入命令regedit，如下图所示。



Step 02 单击“确定”按钮，即可打开“注册表编辑器”窗口，在其中查看注册表信息，如下图所示。



在“注册表编辑器”窗口中可以看到注册表包含有HKEY_LOCAL_MACHINE、HKEY_CLASSES_ROOT、HKEY_CURRENT_USER、HKEY_USERS以及HKEY_CURRENT_CONFIG五个注册表根项，其名称和作用如下表所示。

表　注册表根项名称及其作用

根 项 名 称	作　　用
HKEY_LOCAL_MACHINE	包含关于本地计算机系统的信息，包括硬件和操作系统数据，如总线类型、系统内存、设备驱动程序和启动控制数据
HKEY_CLASSES_ROOT	包含由各种OLE技术使用的信息和文件类别关联数据。如果在HKEY_LOC AL_MACHINE\SOFTWARE\Classes或HKEY_CURRENT_USER\ SOFTW ARE\Classes中存在某个键或值，则对应键或值将出现在HKEY_CLASSES _ROOT中
HKEY_CURRENT_USER	包含当前登录用户的配置文件，包括环境变量、桌面设置、网络连接、打印机和程序首选项。这些信息与用户的配置文件相关联
HKEY_USERS	包含关于动态加载的用户配置文件和默认的配置文件的信息，该信息同时出现在HKEY_CURRENT_USER中
HKEY_CURRENT_CONFIG	包含在启动时由本地计算机系统使用的硬件配置文件的相关信息

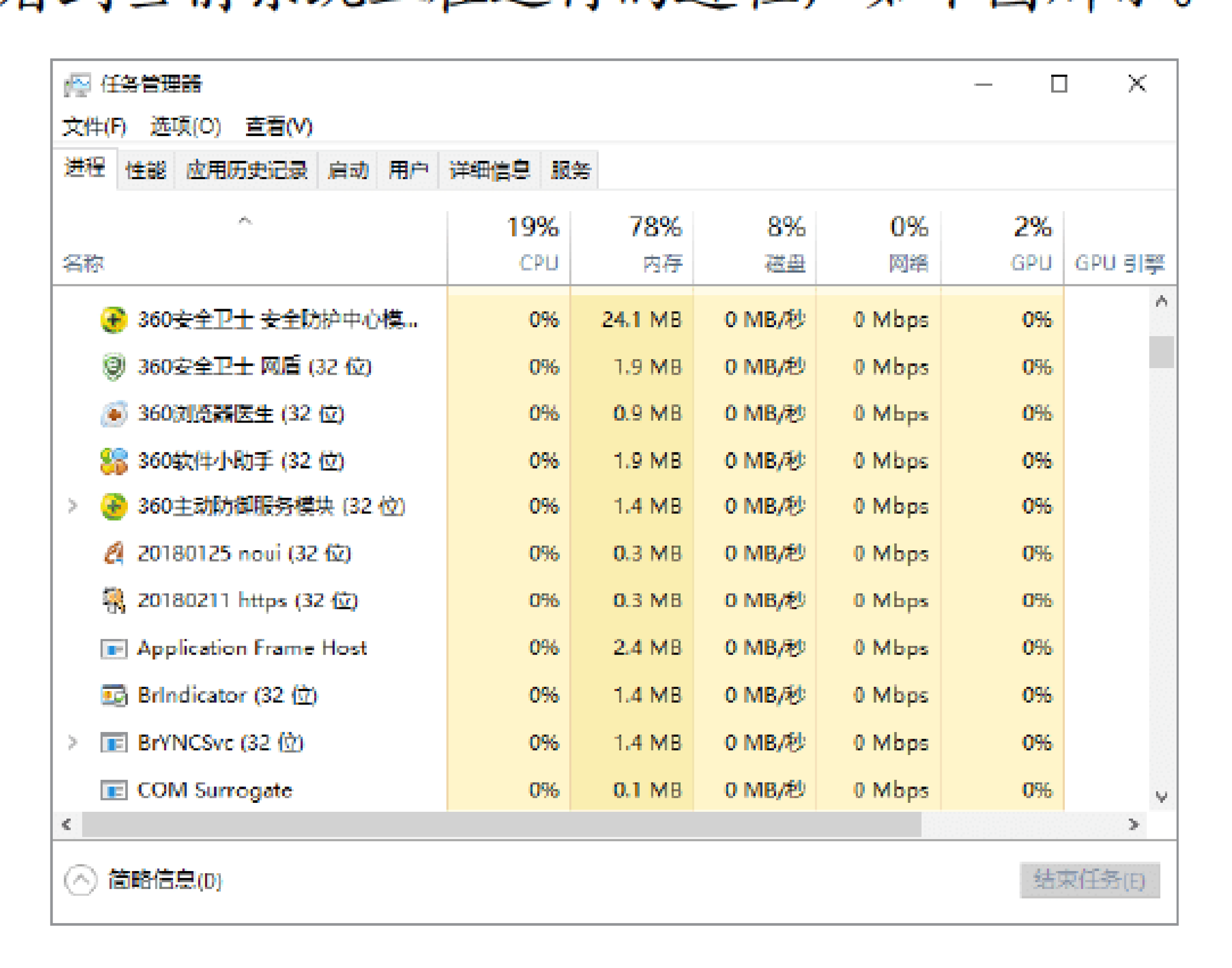
实战5：获取系统进程信息

在Windows 10系统中，可以在“Windows任务管理器”窗口中获取系统进程。具体的操作步骤如下。

Step 01 在Windows 10系统桌面中，单击“开始”按钮，在弹出的菜单列表中选择“任务管理器”选项，如下图所示。



Step 02 打开“任务管理器”窗口，在其中即可看到当前系统正在运行的进程，如下图所示。

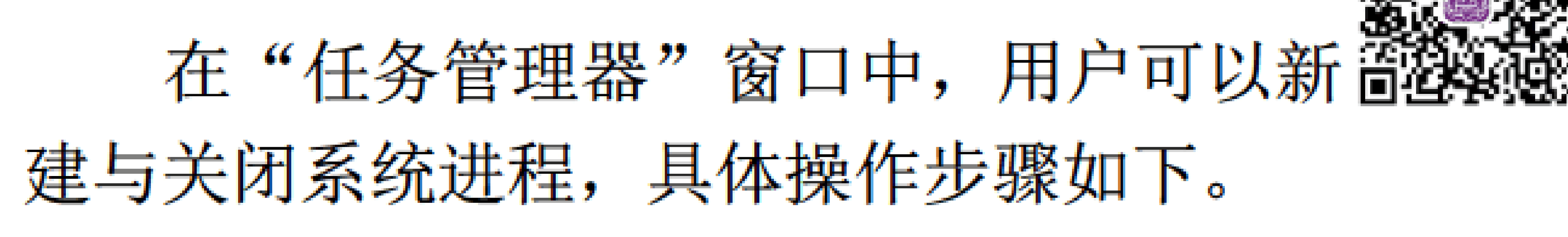




> 提示：在Windows 10系统桌面上，按Ctrl+Del+Alt组合键，在打开的工作界面中单击“任务管理器”链接，即可打开“任务管理器”窗口，在其中查看系统进程。

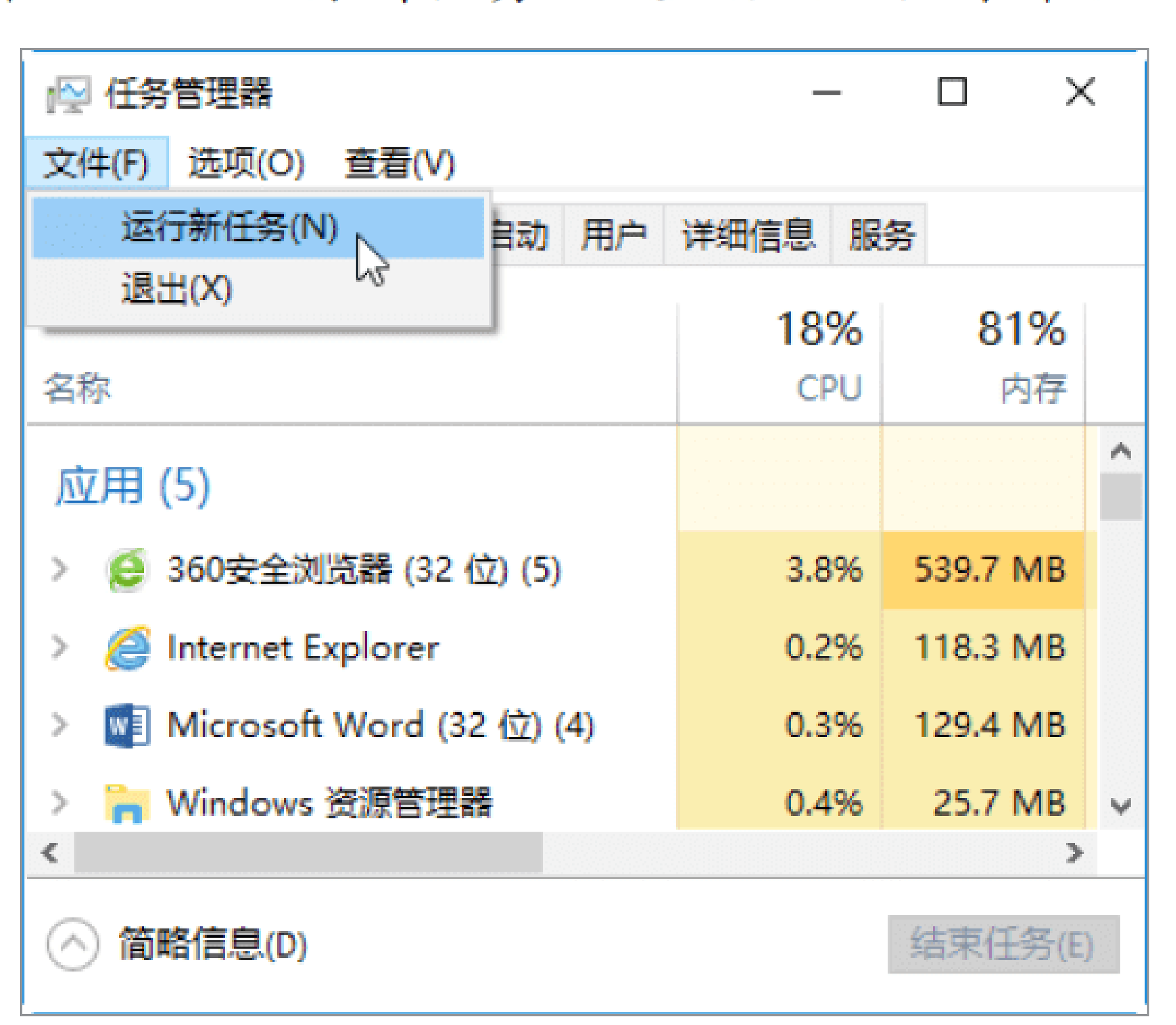
1.4　实战演练

实战演练1——新建与关闭系统进程

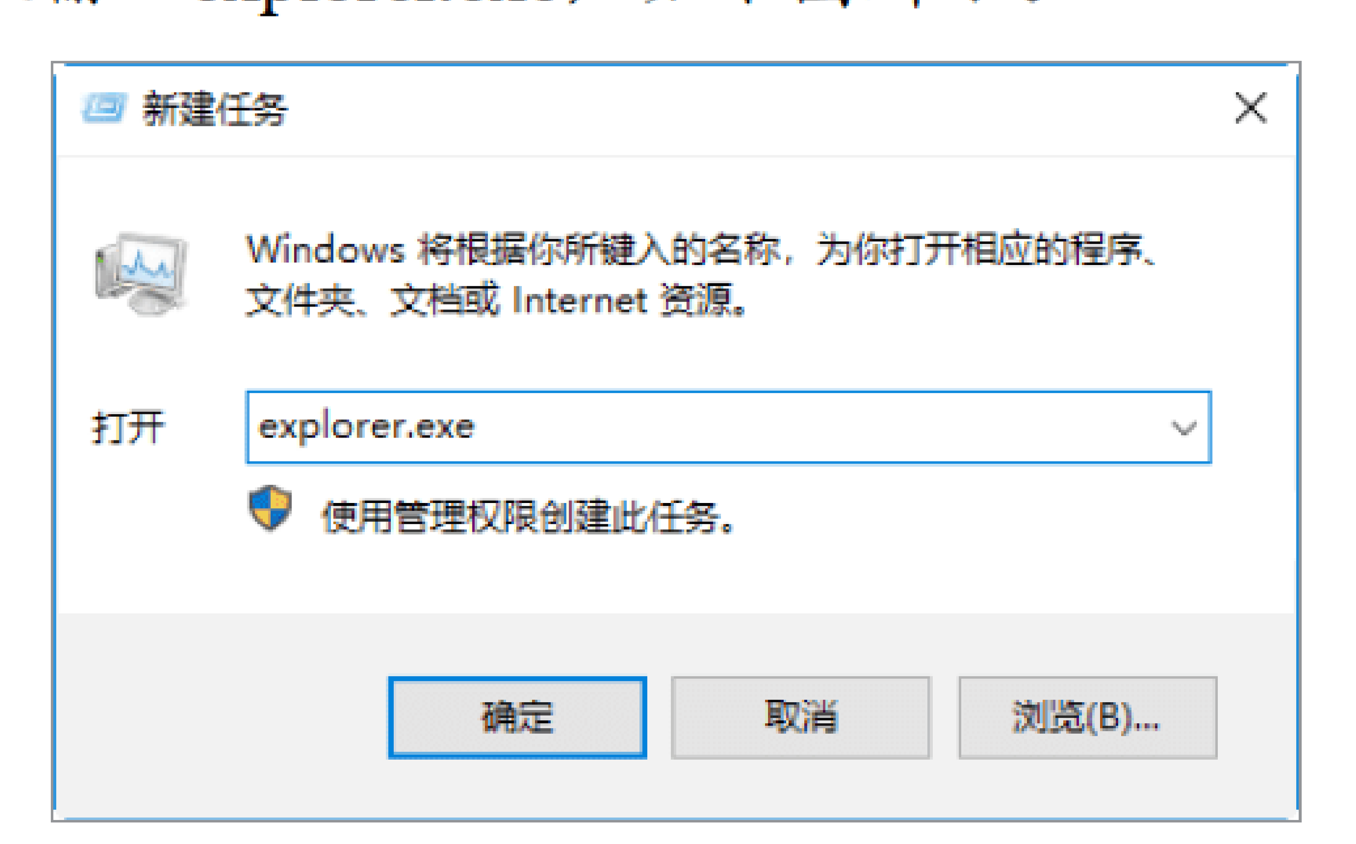


在“任务管理器”窗口中，用户可以新建与关闭系统进程，具体操作步骤如下。

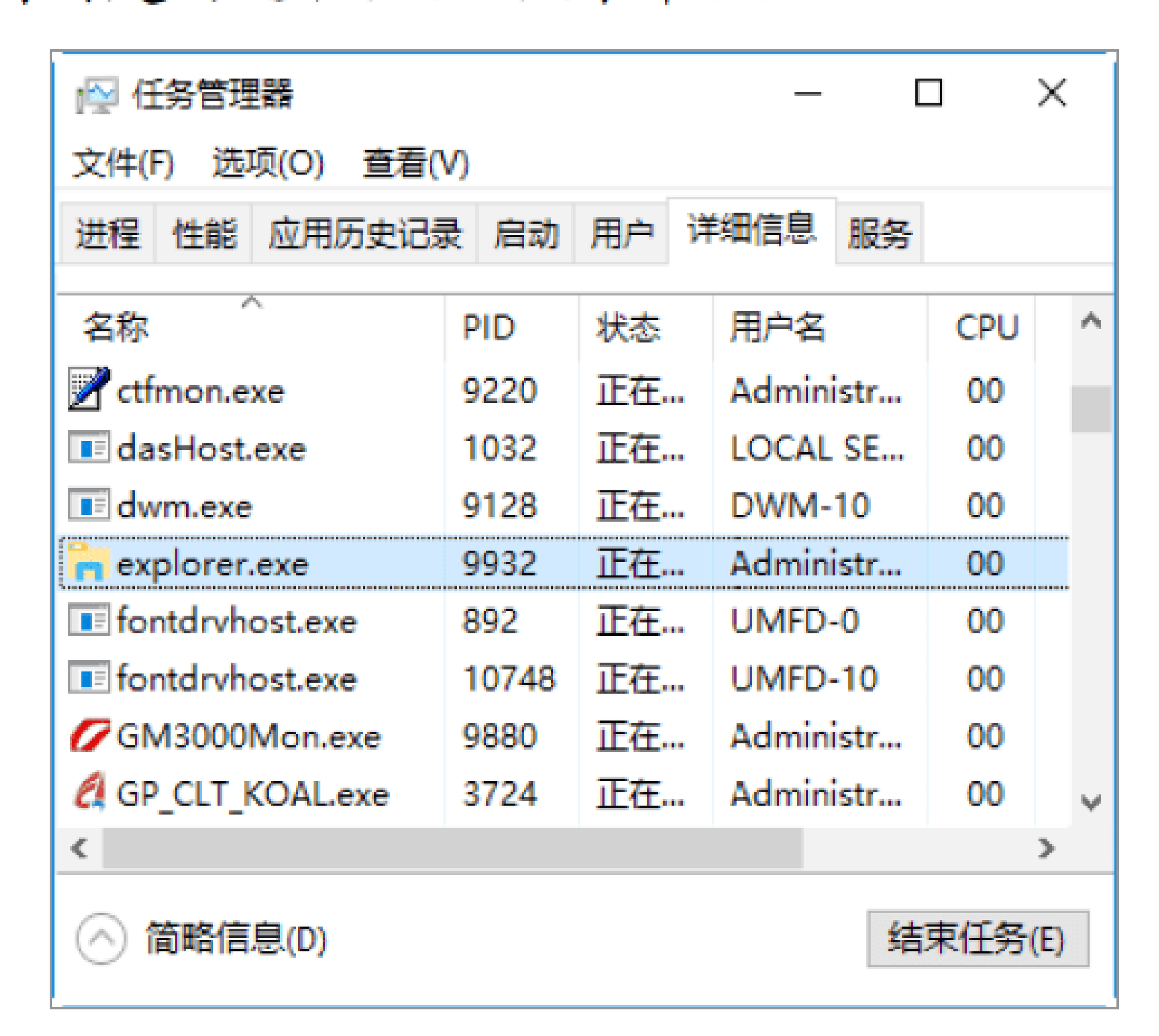
Step 01 在“任务管理器”窗口中选择“文件”→“运行新任务”选项，如下图所示。



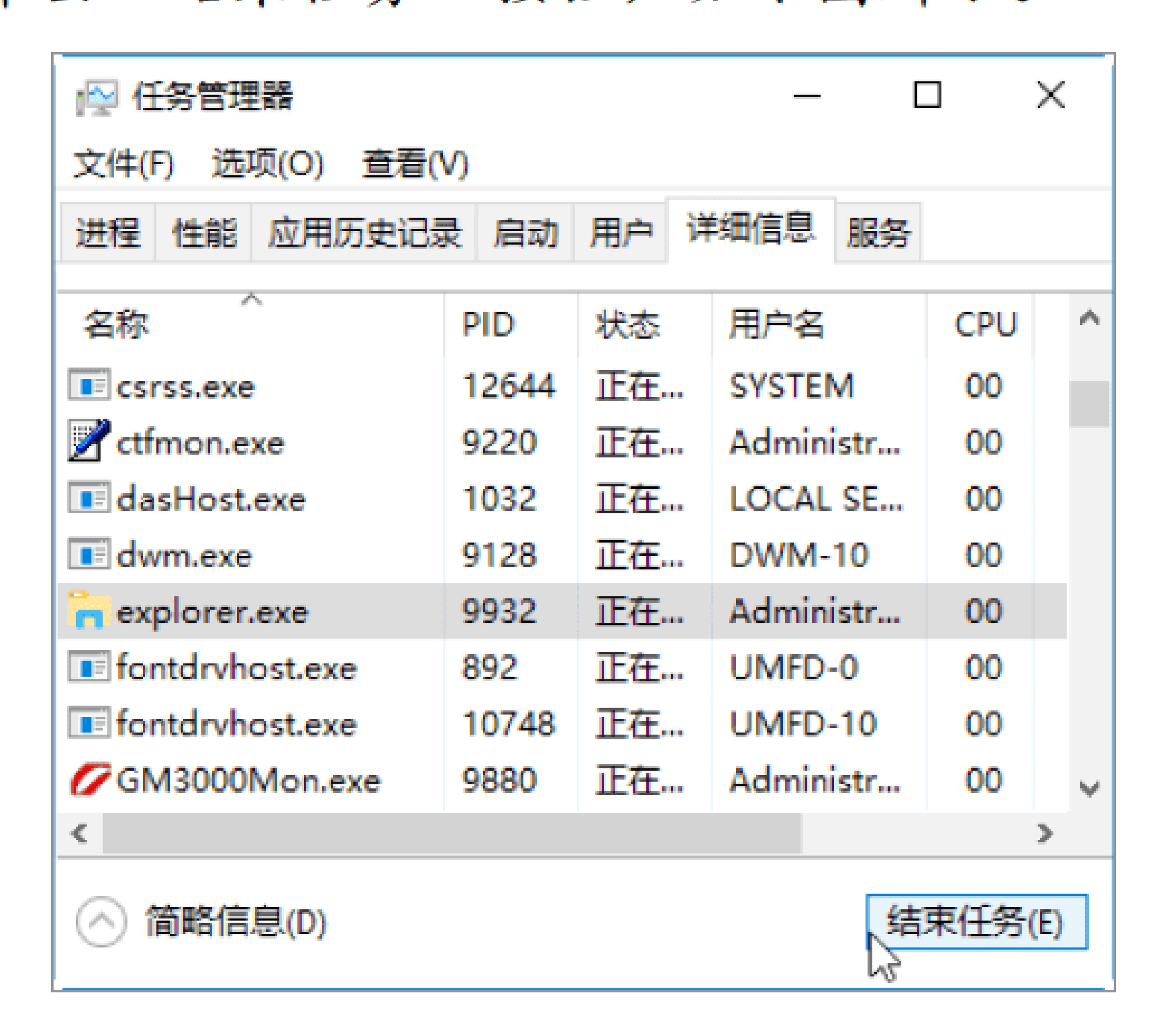
Step 02 打开“新建任务”对话框，在“打开”文本框中输入新建的进程名称，如这里输入explorer.exe，如下图所示。



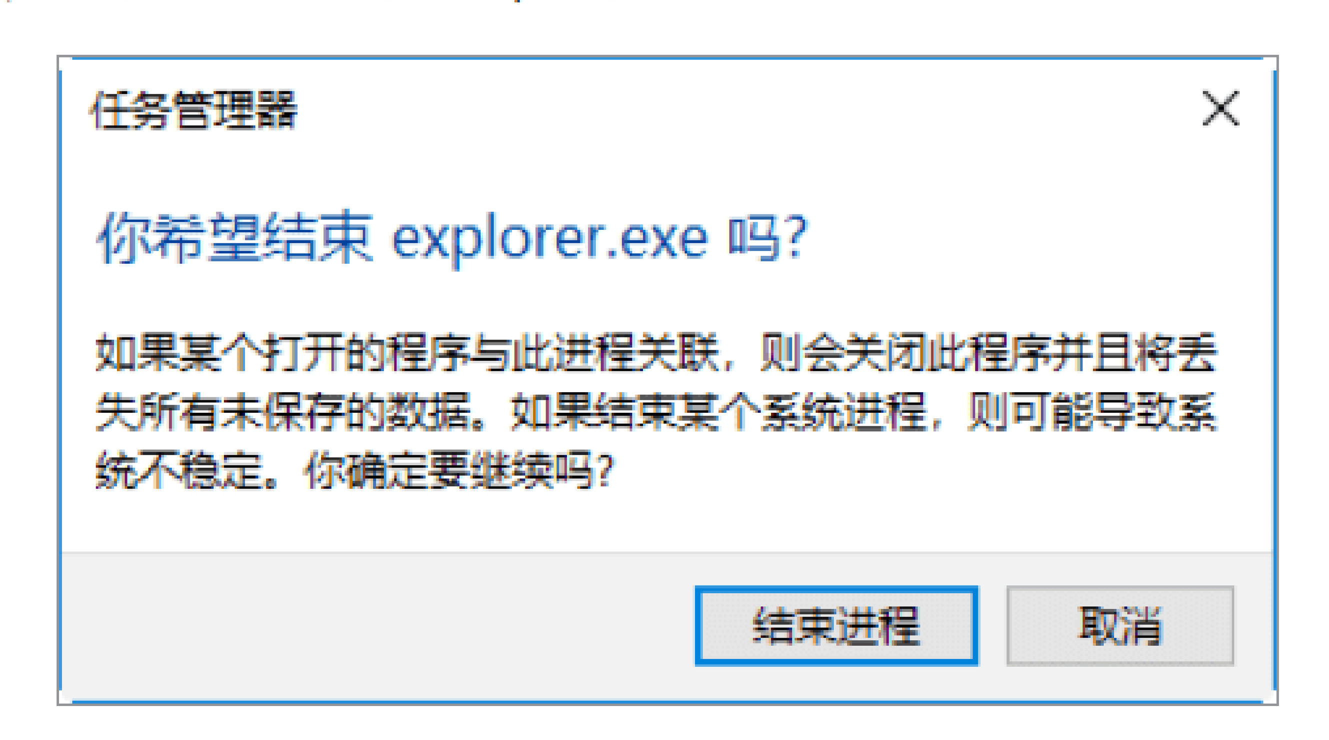
Step 03 单击“确定”按钮，即可创建一个新的进程，在“详细信息”选项卡中可以看到创建的进程，如下图所示。



Step 04 如果想要结束某个进程，用户可以在“任务管理器”窗口选中要结束的进程，单击“结束任务”按钮，如下图所示。



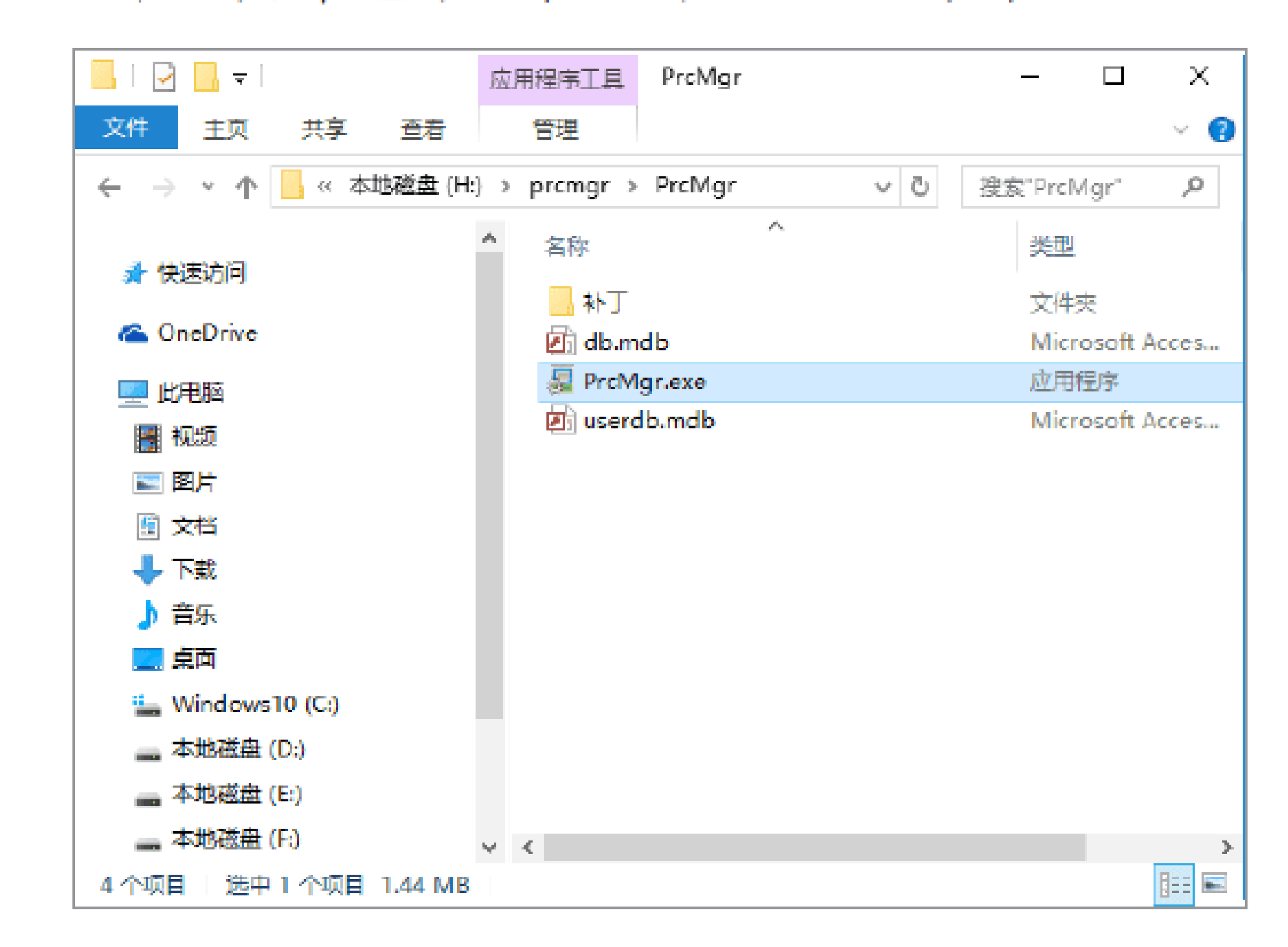
Step 05 随即会弹出“任务管理器”警告对话框，如下图所示。单击“结束进程”按钮，即可关闭该进程。此时如果单击“取消”按钮，则结束进程。



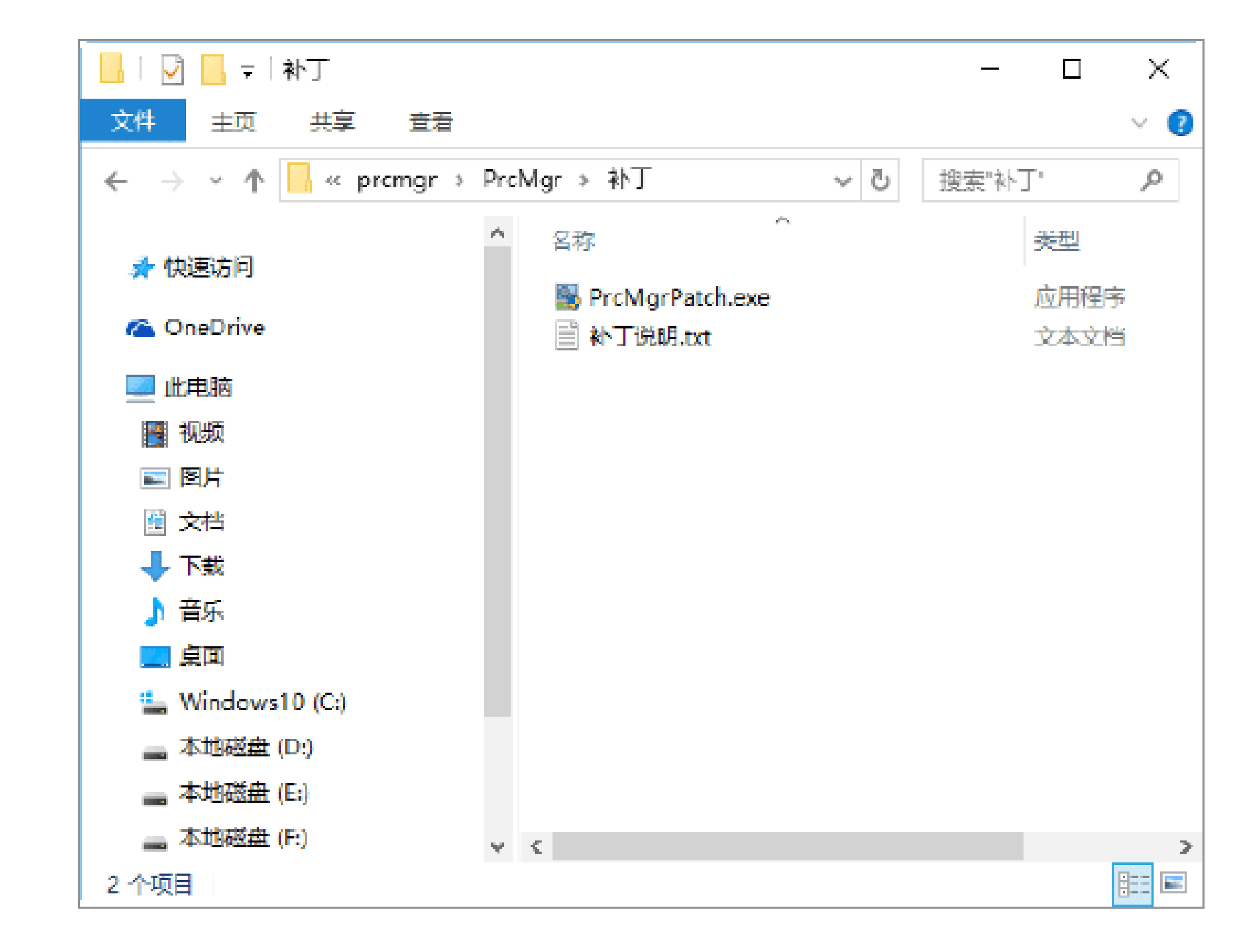
实战演练2——全面管理系统进程信息

使用Windows进程管理器可以对系统进程进行更加全面的管理，其最大的特点是包含了几乎全部的Windows系统进程和大量的常用软件进程。使用Windows进程管理器管理进程的操作步骤如下。

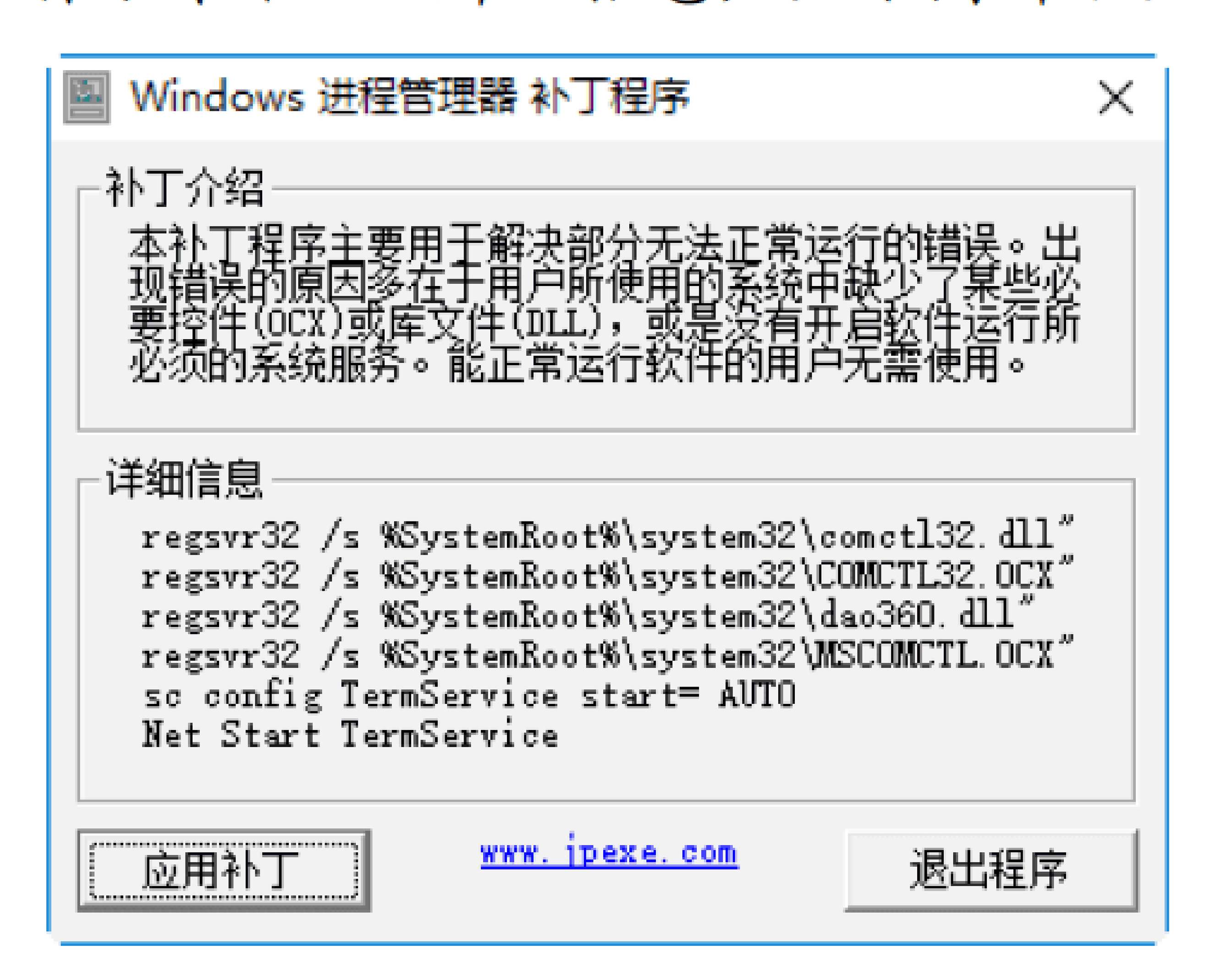
Step 01 下载并解压缩“Windows进程管理器”软件，其中包含4个文件，如下图所示。



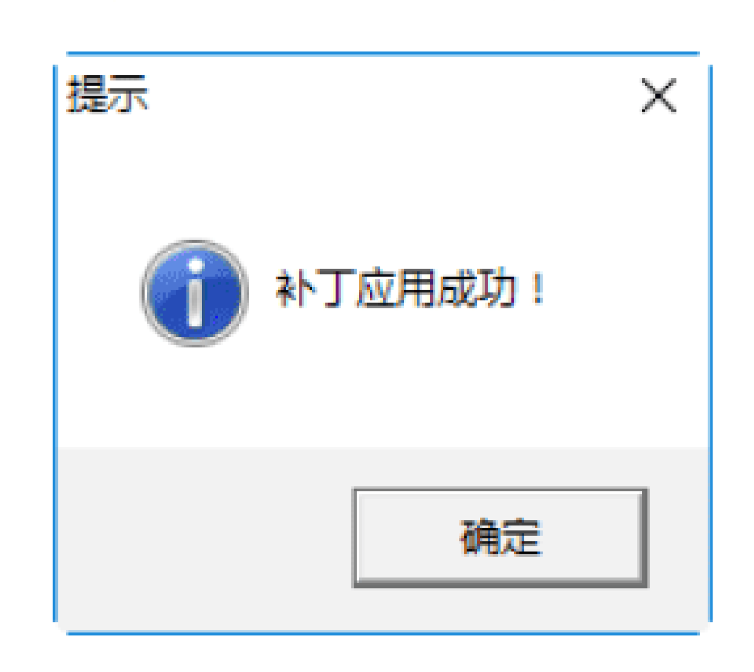
Step 02 双击“补丁”文件夹，打开“补丁”文件夹，在其中可以看到Windows进程管理器的补丁程序和补丁说明文件，如下图所示。



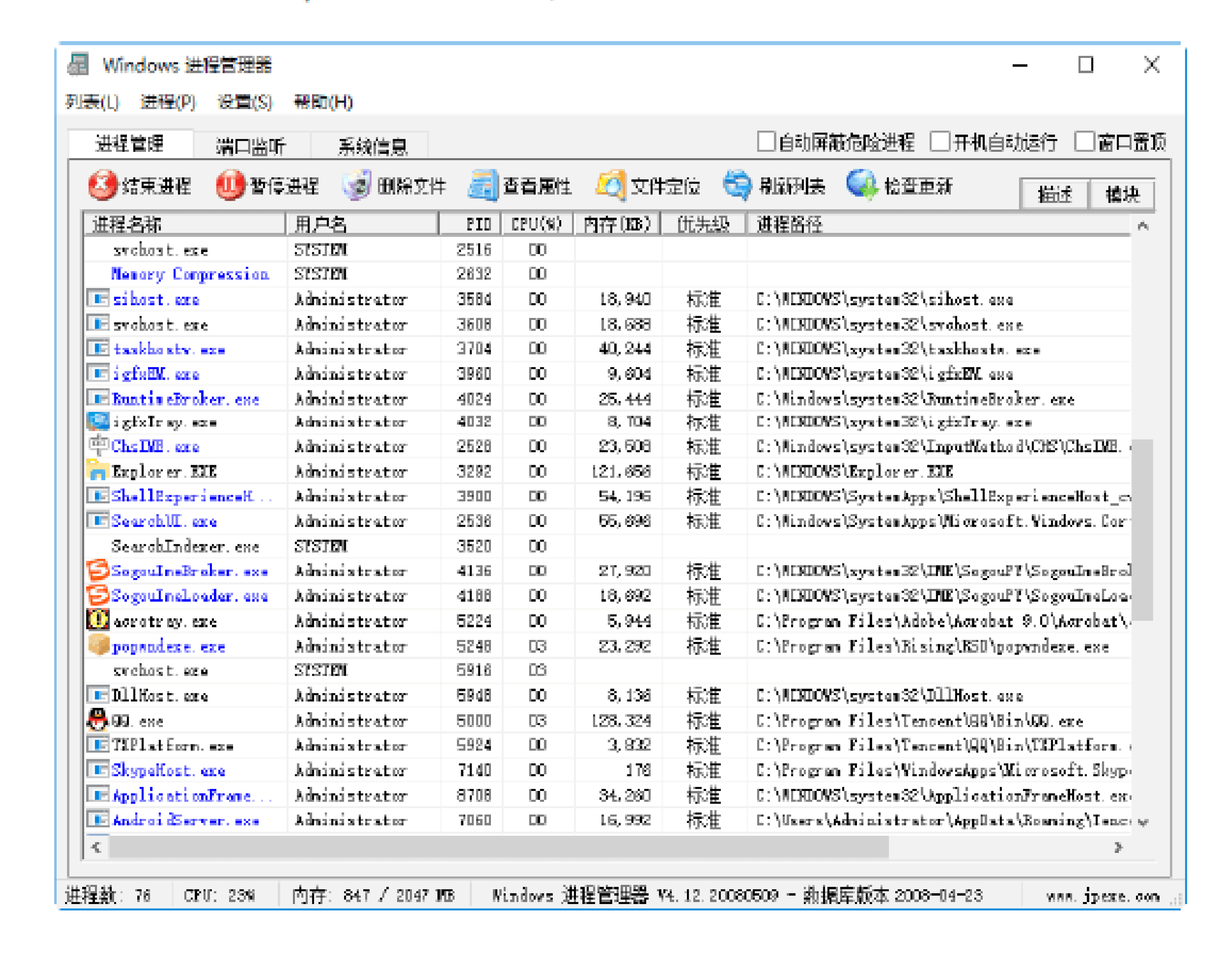
Step 03 双击补丁应用程序，打开“Windows进程管理器 补丁程序”对话框，在其中显示补丁介绍以及详细信息，如下图所示。



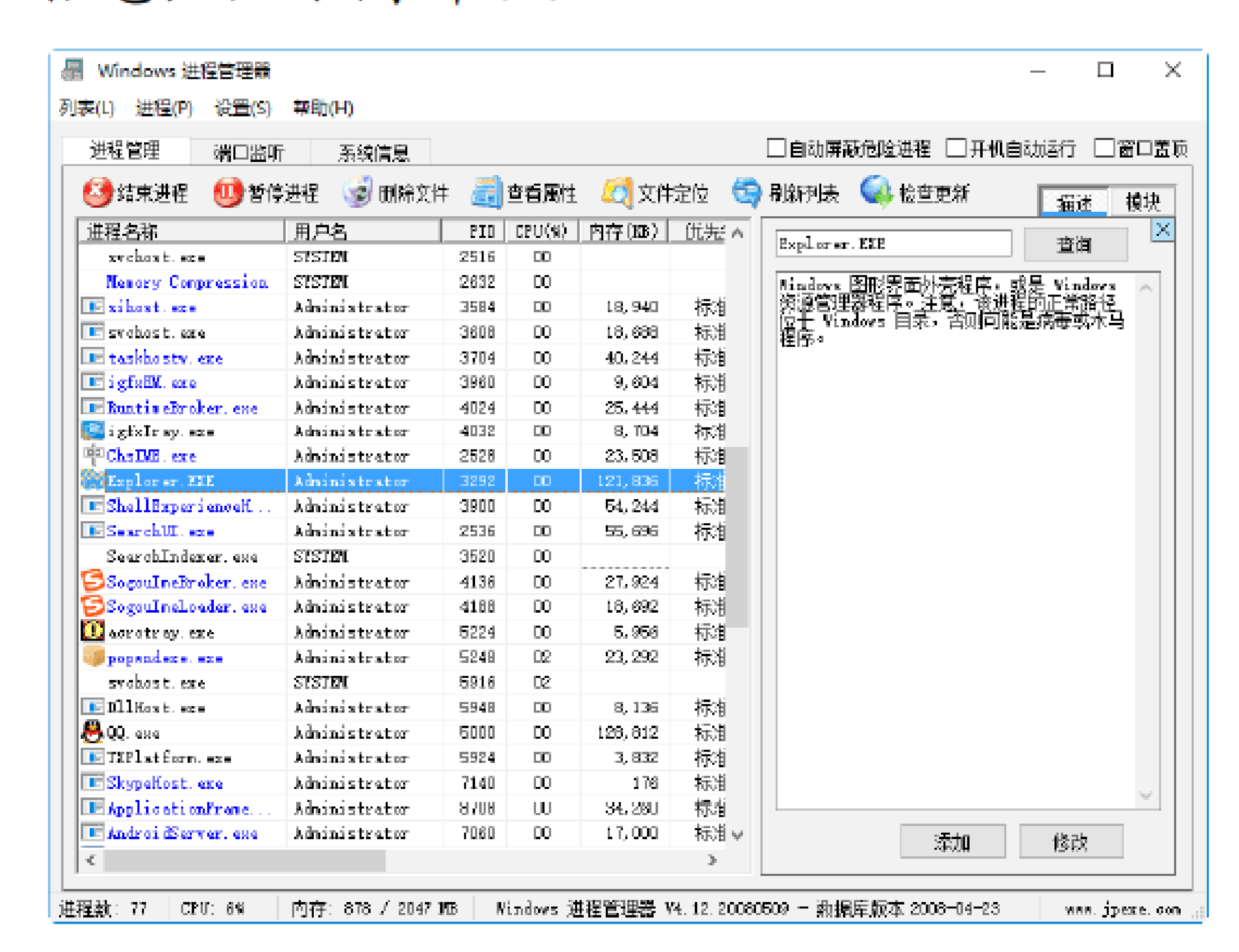
Step 04 单击“应用补丁”按钮，即可应用补丁程序，并弹出“提示”对话框，提示用户补丁应用成功，如下图所示。



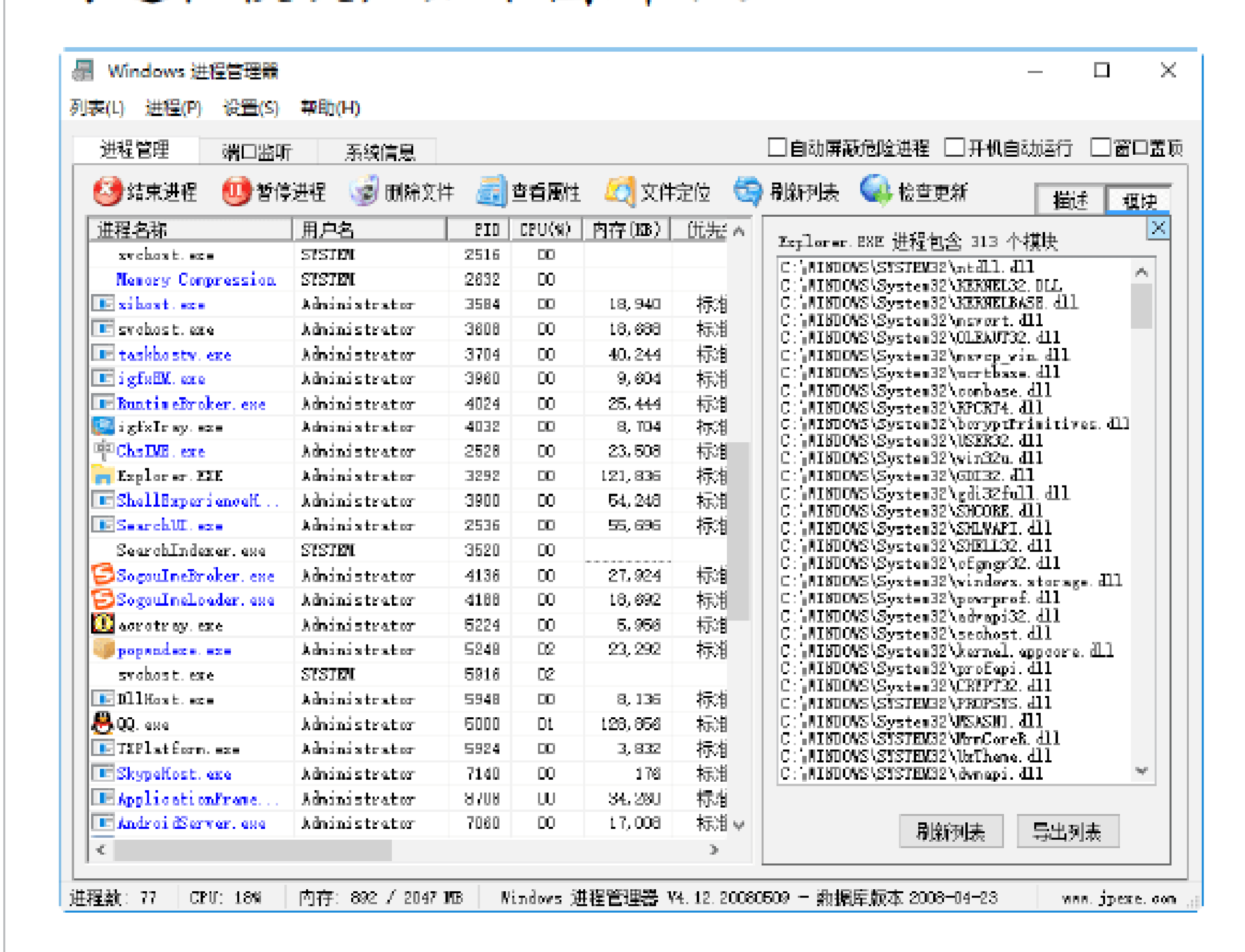
Step 05 单击“确定”按钮，关闭“提示”对话框。双击Windows进程管理器启动程序，打开“Windows进程管理器”窗口，如下图所示。其中显示了系统当前正在运行的所有进程，与“Windows任务管理器”窗口中的进程列表是完全相同的。



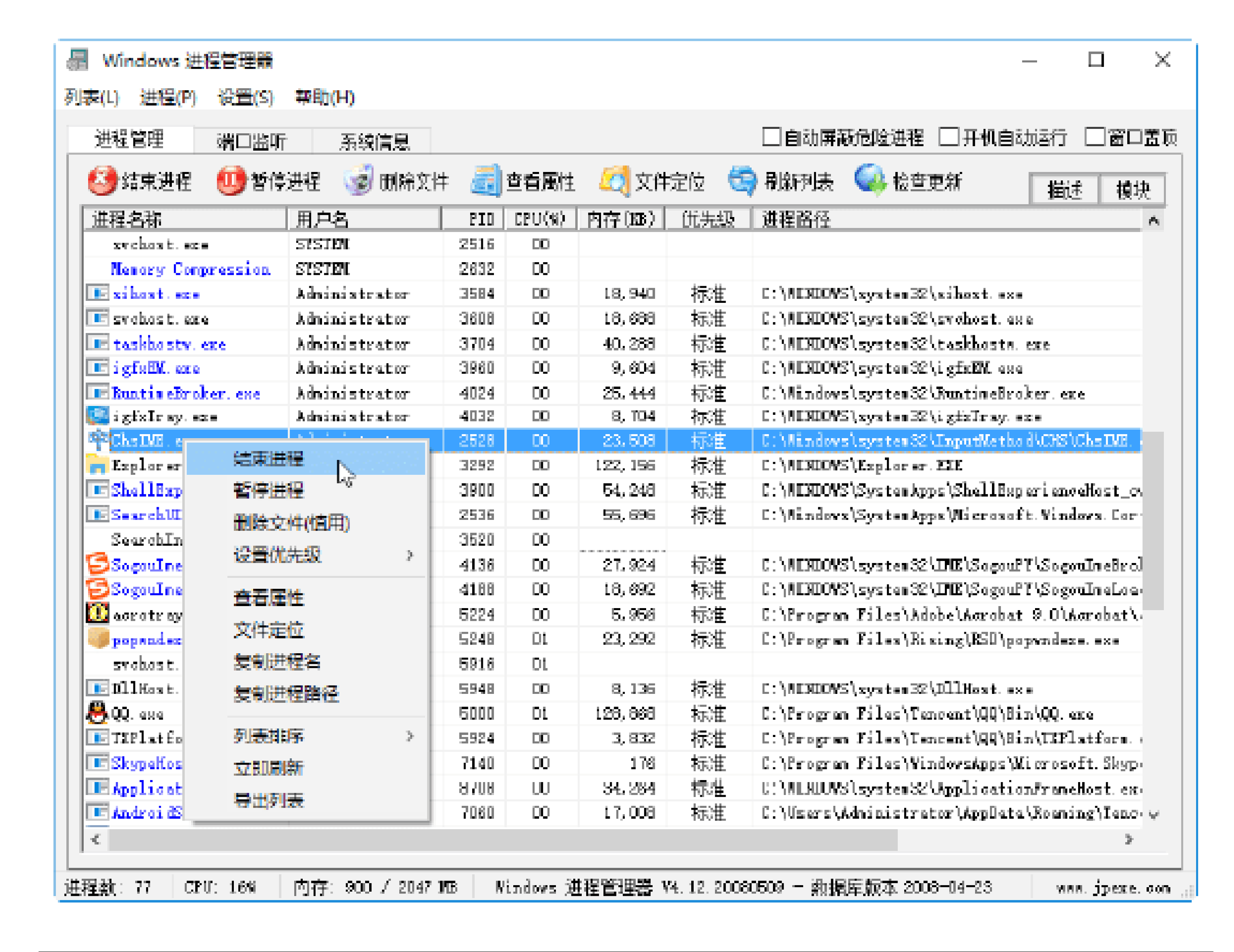
Step 06 在列表中选择其中一个进程选项，单击“描述”按钮，即可看到该进程的详细信息，如下图所示。



Step 07 单击“模块”按钮，即可查看该进程的进程模块，如下图所示。



Step 08 在进程列表中右击某个进程，在弹出的快捷菜单中可以进行结束、暂停、查看属性、删除文件等操作，如下图所示。



提示：按进程的安全等级进行了区分。①黑色表示正常进程（正常的系统或应用程序进程，安全）；

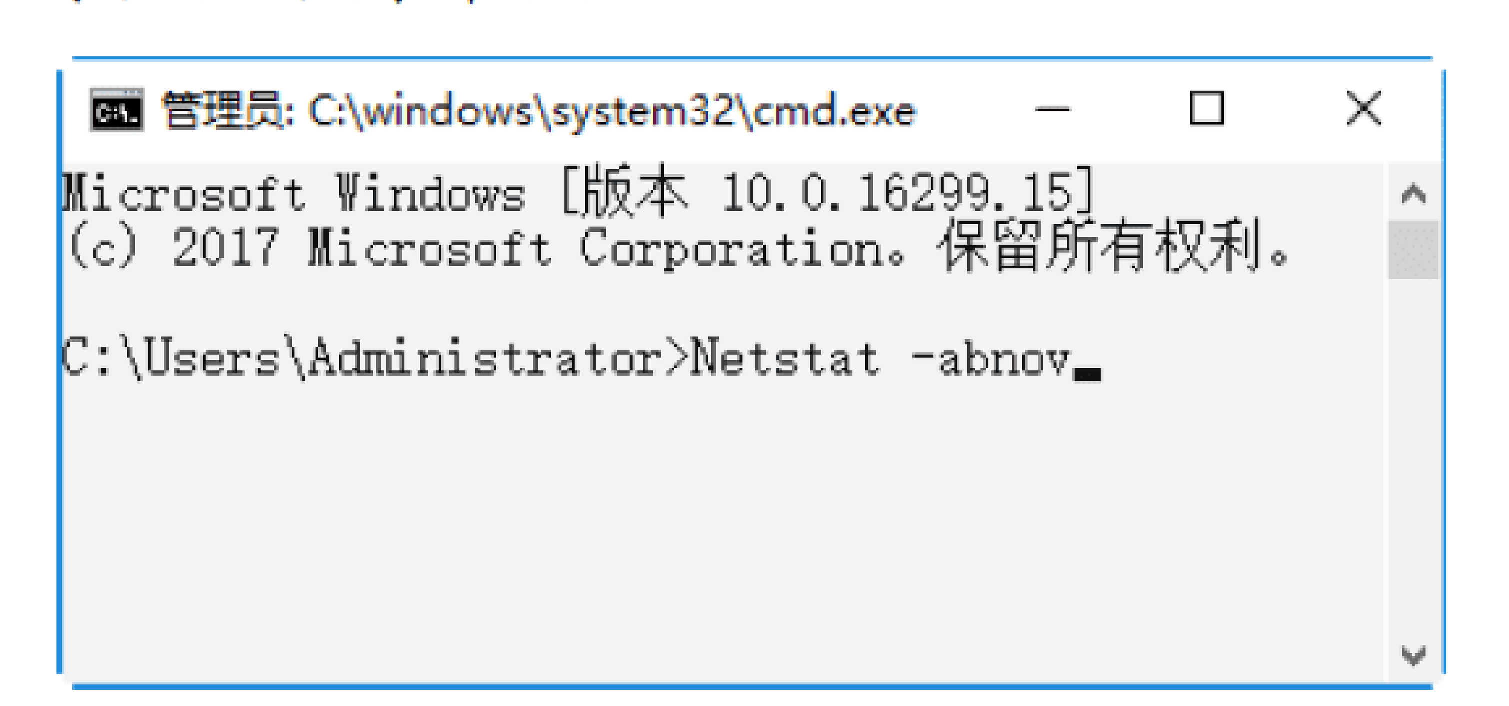
② 蓝色表示可疑进程（容易被病毒或木马利用的正常进程，需要留心）；
③ 红色表示病毒&木马进程（危险）。

1.5　小试身手

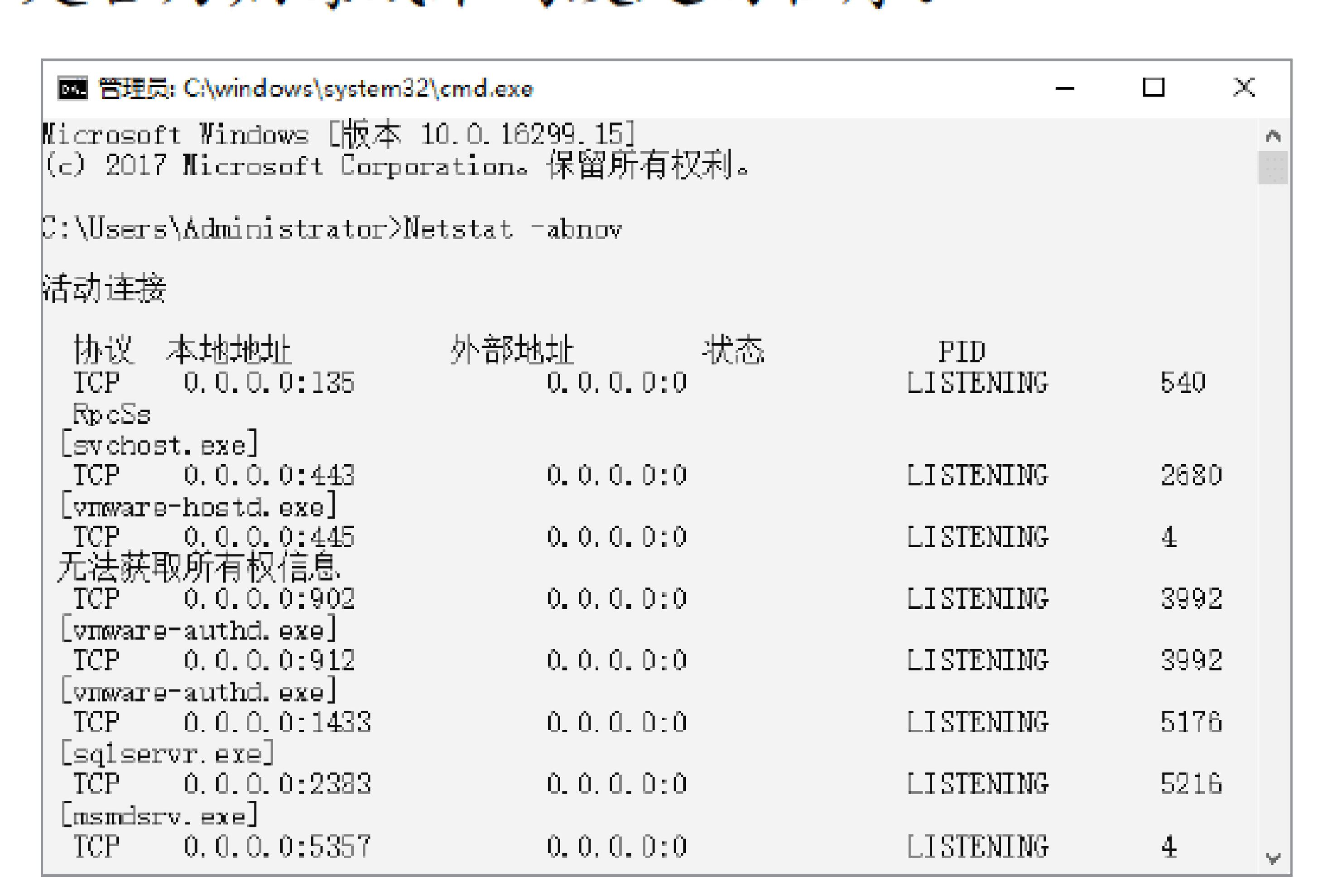
练习1：查看进程起始程序

用户通过查看进程的起始程序，可以判断哪些进程是恶意进程。查看进程起始程序的具体操作步骤如下。

Step 01 在“命令提示符”窗口中输入查看Svchost进程起始程序的Netstat –abnov命令，如下图所示。



Step 02 按Enter键，即可在反馈的信息中查看每个进程的起始程序或文件列表，如下图所示，这样就可以根据相关的知识来判断是否为病毒或木马发起的程序。



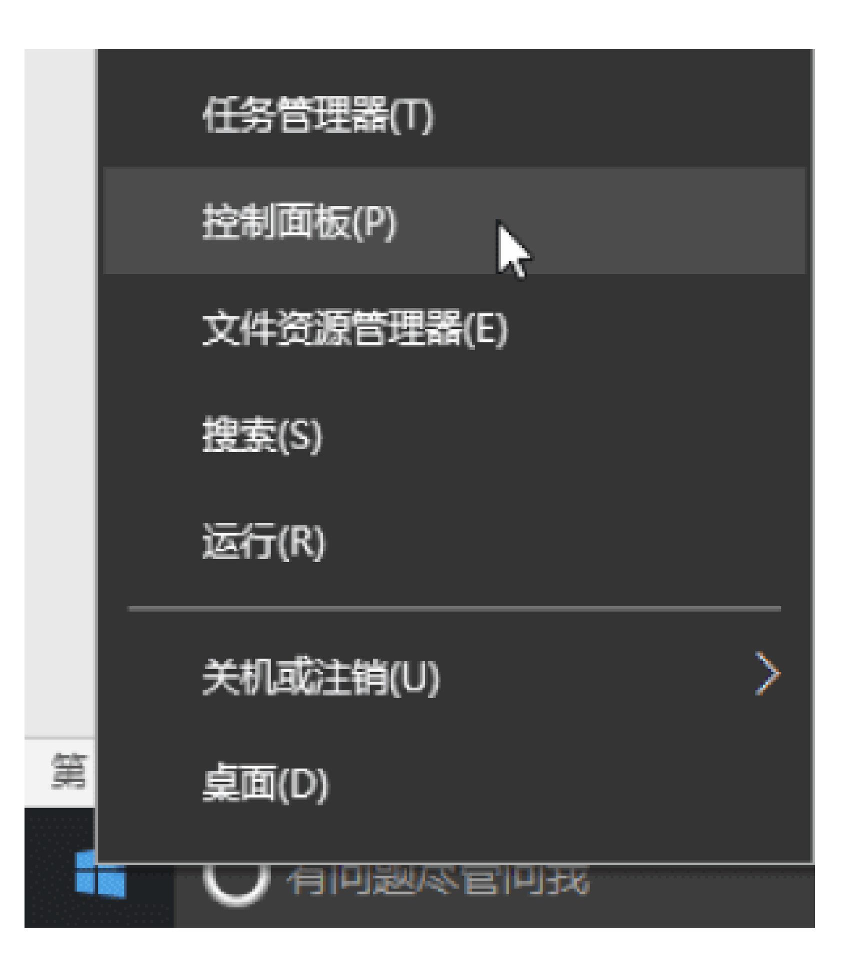


练习2：关闭不必要的端口

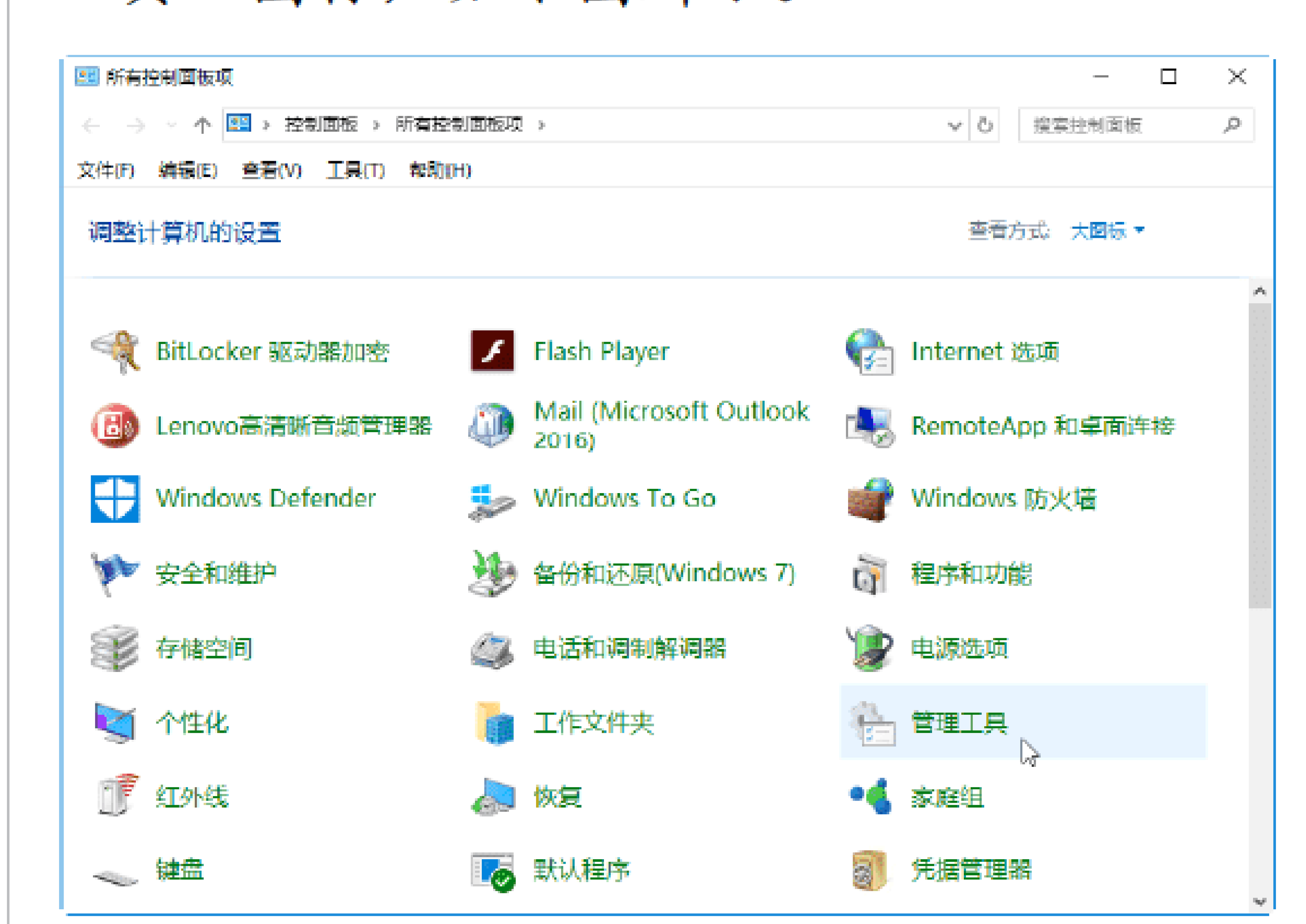
默认情况下，计算机系统中有很多没有用或不安全的端口是开启的，这些端口很容易被黑客利用。为保障系统的安全，可以将这些不用的端口关闭。关闭端口的方式有多种，这里介绍通过关闭无用服务来关闭不必要的端口。

以关闭Branch Cache服务为例，具体操作步骤如下。

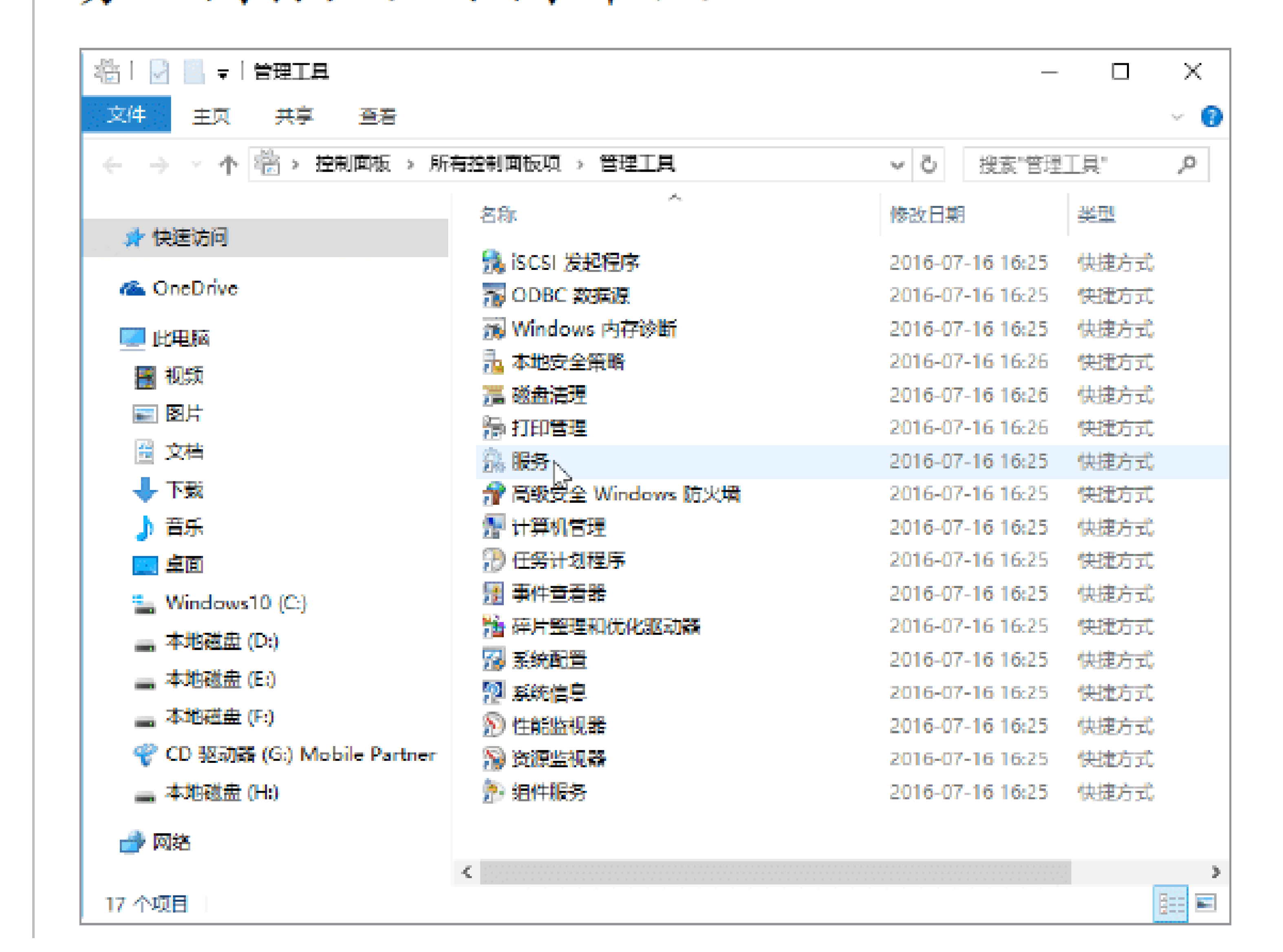
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”选项，如下图所示。



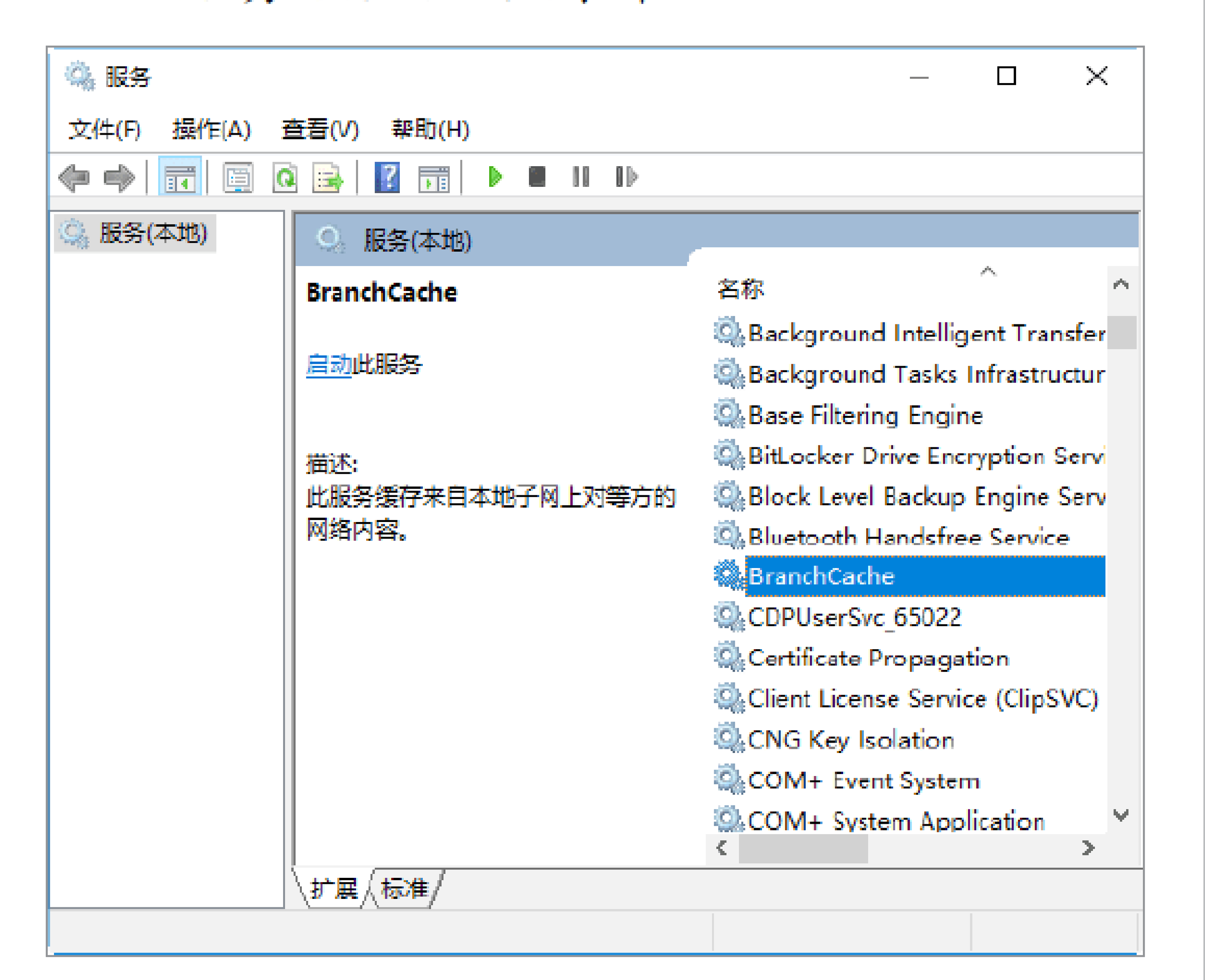
Step 02 打开“控制面板”窗口，双击“管理工具”图标，如下图所示。



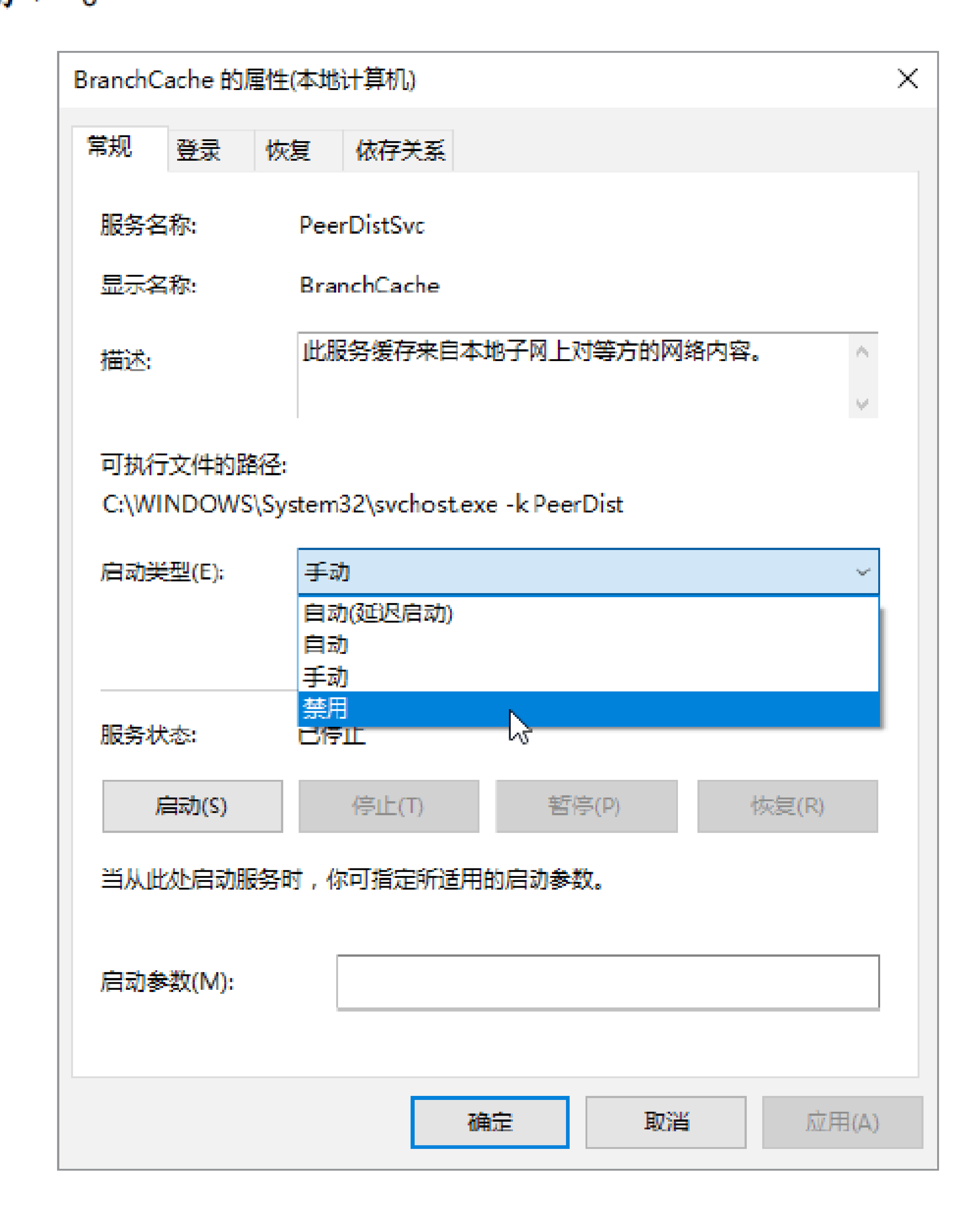
Step 03 打开“管理工具”窗口，双击“服务”图标，如下图所示。



Step 04 打开“服务”窗口，找到BranchCache服务项，如下图所示。



Step 05 双击该服务项，弹出“BranchCache的属性”对话框，在“启动类型”下拉列表框中选择“禁用”选项，如下图所示，然后单击“确定”按钮，禁用该服务项的端口。



第2章　搭建网络安全测试环境

安全测试环境是黑客攻防实战必备的内容，也是安全工作者需要了解和掌握的内容。另外，对于黑客初学者来说，在学习过程中需要找到符合条件的目标计算机，并进行模拟攻击，而这些攻击目标并不是初学者能够从网络上搜索到的，这就需要通过搭建网络安全测试环境来解决这个问题。

2.1　认识安全测试环境

所谓安全测试环境就是在已存在的一个系统中，利用虚拟机工具创建出一个内在的虚拟系统，也被称作安全测试环境。该系统与外界独立，但与已存在的系统建有网络关系，该系统中可以进行测试和模拟黑客入侵方式。

2.1.1　什么是虚拟机软件

虚拟机软件是一种可以在一台计算机上模拟出很多台计算机的软件，而且每台计算机都可以运行独立的操作系统，且不相互干扰，实现了一台“计算机”运行多个操作系统的功能，同时还可以将这些操作系统连成一个网络。

常见的虚拟机软件有VMware和Virtual PC两种。VMware是一款功能强大的桌面虚拟计算机软件，支持在主机和虚拟机之间共享数据，支持第三方预设置的虚拟机和镜像文件，而且安装与设置都非常简单。

Virtual PC运用具有最新的Microsoft虚拟化技术，用户可以使用这款软件在同一台计算机上同时运行多个操作系统，操作起来非常简单，用户只需单击一下，便可直接在计算机上虚拟出Windows环境，在该环境中可以同时运行多个应用程序。



2.1.2　什么是虚拟系统

虚拟系统就是在现已有的操作系统的基础上，安装一个新的操作系统或者虚拟出系统本身的文件，该操作系统允许在不重启计算机的基础上进行切换。

创建虚拟系统的好处有以下几种。

（1）虚拟技术是一种调配计算机资源的方法，可以更有效、更灵活地提供和利用计算机资源，降低成本，节省开支。

（2）在虚拟环境里更容易实现程序自动化，有效地减少测试要求和应用程序的兼容性问题，在系统崩溃时更容易实施恢复操作。

（3）虚拟系统允许跨系统进行安装，如在Windows 10的基础上可以安装Linux操作系统。

2.2　安装与创建虚拟机

对于网络安全初学者，使用虚拟机构建网络安全测试环境是一个非常好的选择，这样既可以快速搭建测试环境，同时还可以快速还原之前快照，避免错误操作造成系统崩溃。

实战1：下载虚拟机软件

虚拟机使用之前，需要从官网上下载虚拟机软件VMware。具体的操作步骤如下。

Step 01 使用浏览器打开虚拟机官方网站https：//my.vmware.com/cn，进入虚拟机官网页面，如下图所示。



Step 02 这里需要注册一个账号，用户可以注册一个账号，VMware支持中文页面，正常注册即可。注册完成后，进入“所有下载”页面，并切换到“所有产品”选项卡，如下图所示。

所有下载

我的产品 | 所有产品 | 产品列表（A 到 Z）

Step 03 在下拉页面找到VMware Workstation Pro对应选项，单击右侧的“查看下载组件”超链接，如下图所示。

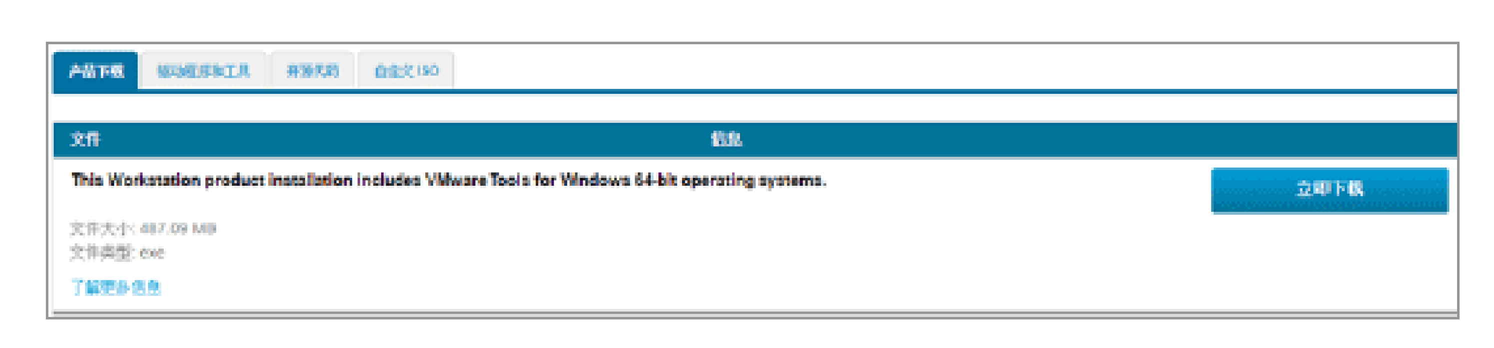
VMware Workstation Pro　　查看下载组件 | 驱动程序和工具

Step 04 进入VMware下载页面，在其中选择Windows版本，单击右侧“转至下载”超链接，如下图所示。

产品下载 | 驱动程序和工具 | 开源代码 | 自定义 ISO

产品	发行日期	
VMware Workstation Pro 14.1.3 for Windows		
VMware Workstation 14.1.3 Pro for Windows	2018-08-14	转至下载
VMware Workstation Pro 14.1.3 for Linux		
VMware Workstation 14.1.3 Pro for Linux	2018-08-14	转至下载

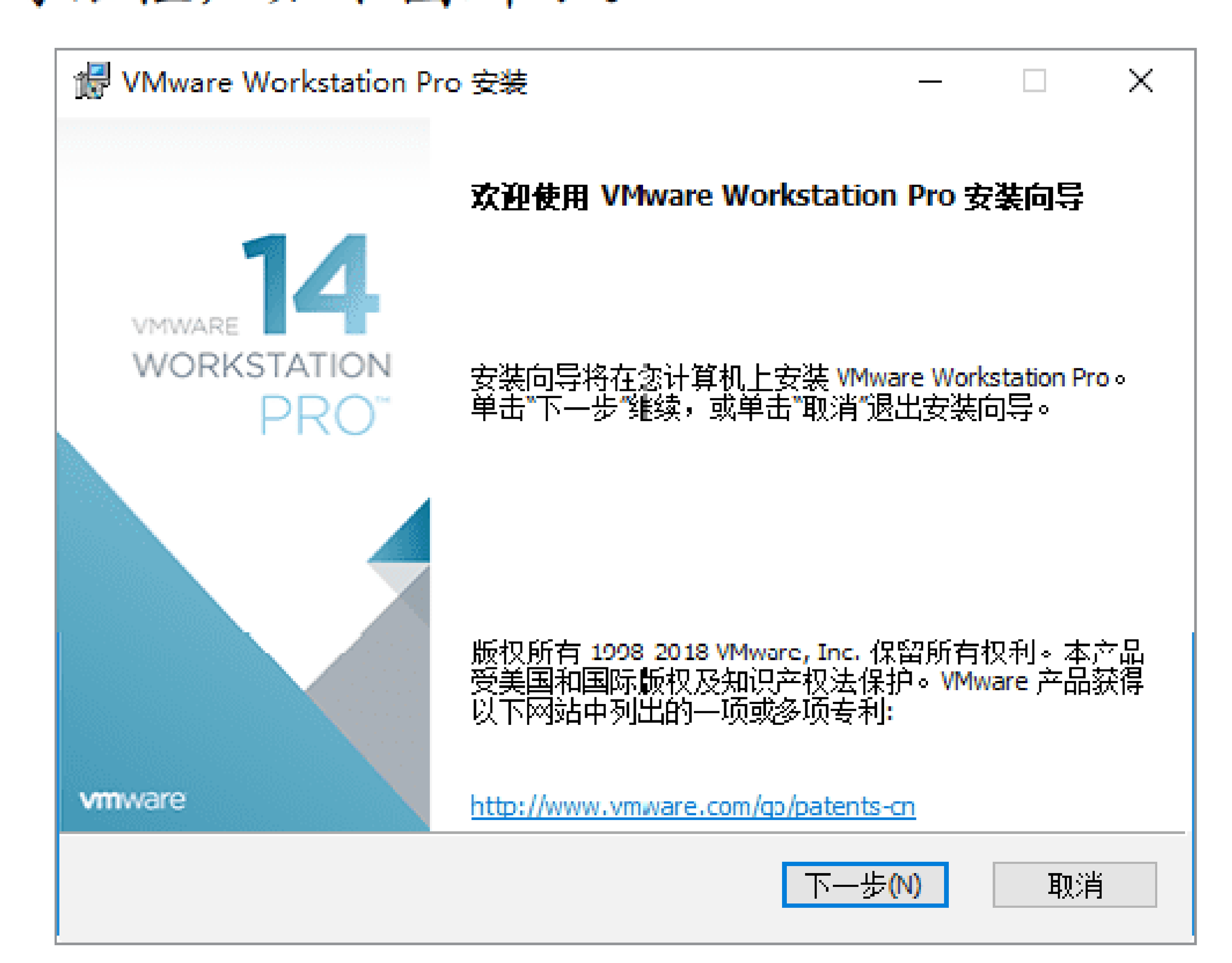
Step 05 跳转至下载页面，单击“立即下载”按钮进行下载，如下图所示。



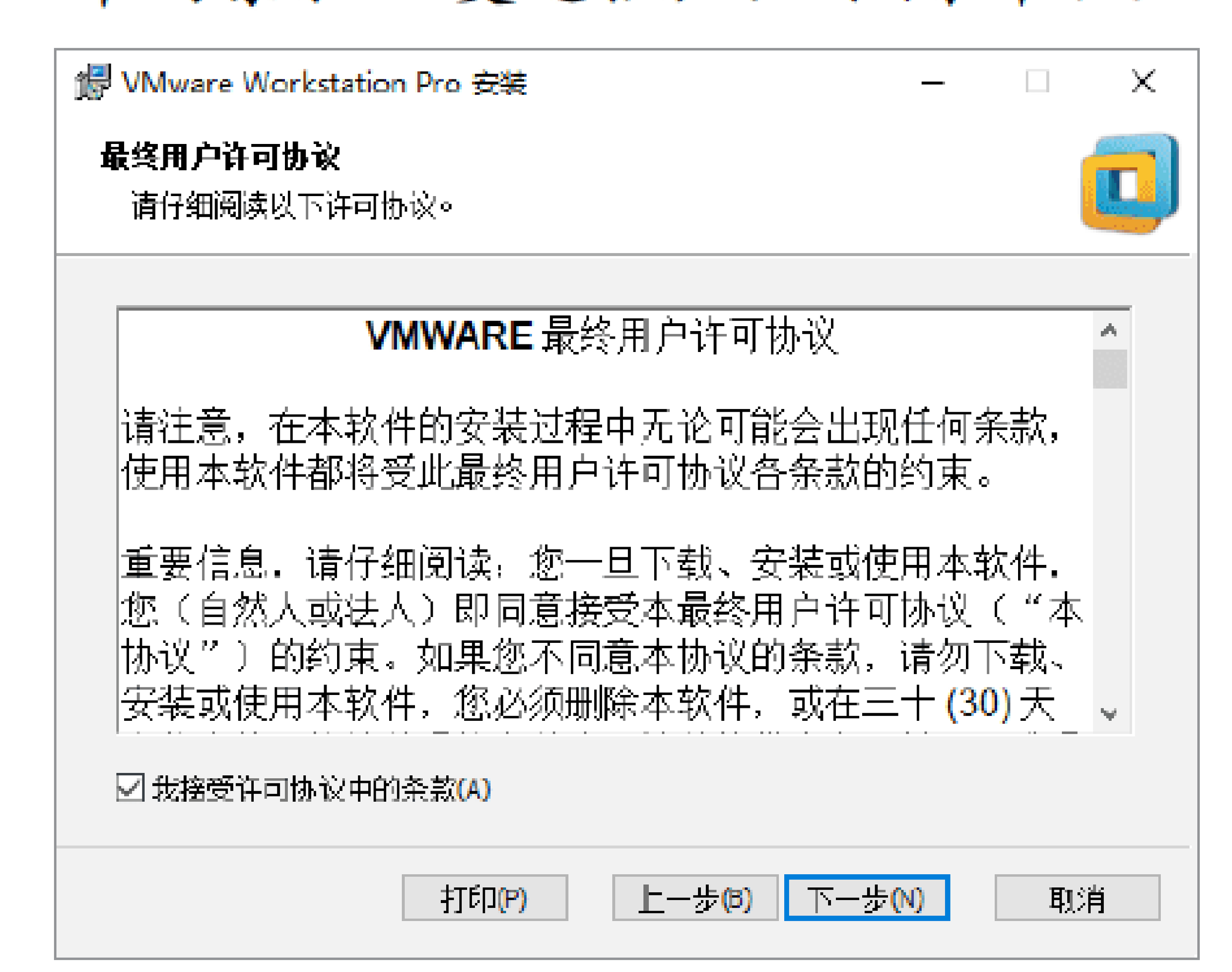
实战2：安装虚拟机软件

虚拟机软件下载完成后，接下来就可以安装虚拟机软件了。这里下载的是目前最新版本VMware-workstation-full-14.1.2-9474260.exe，用户可根据实际情况选择当前最新版本下载即可。安装虚拟机的具体操作步骤如下。

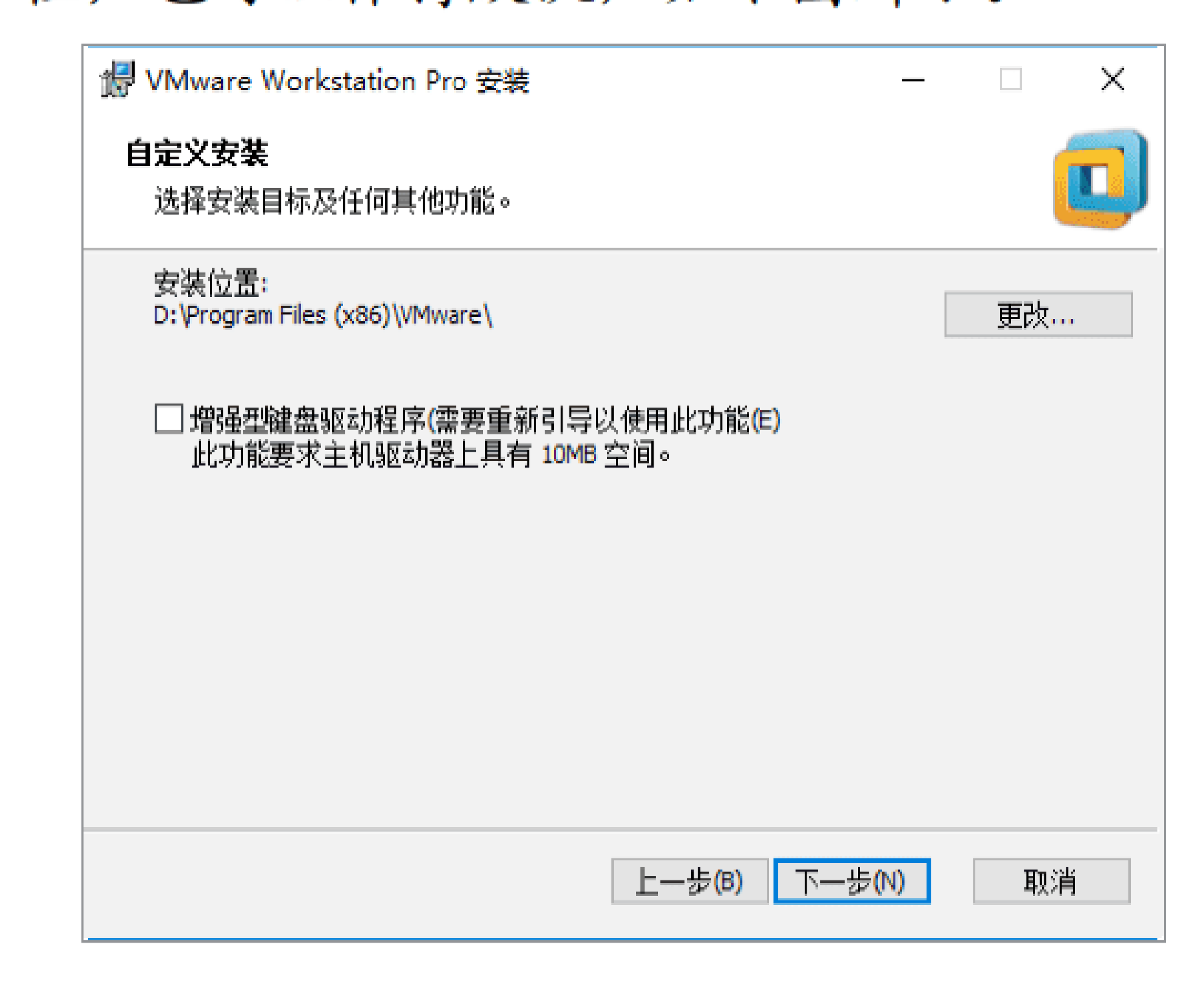
Step 01 双击下载的VMware安装软件，进入“欢迎使用VMware Workstation Pro安装”对话框，如下图所示。



Step 02 单击“下一步”按钮，进入“最终用户许可协议”对话框，勾选“我接受许可协议中的条款”复选框，如下图所示。

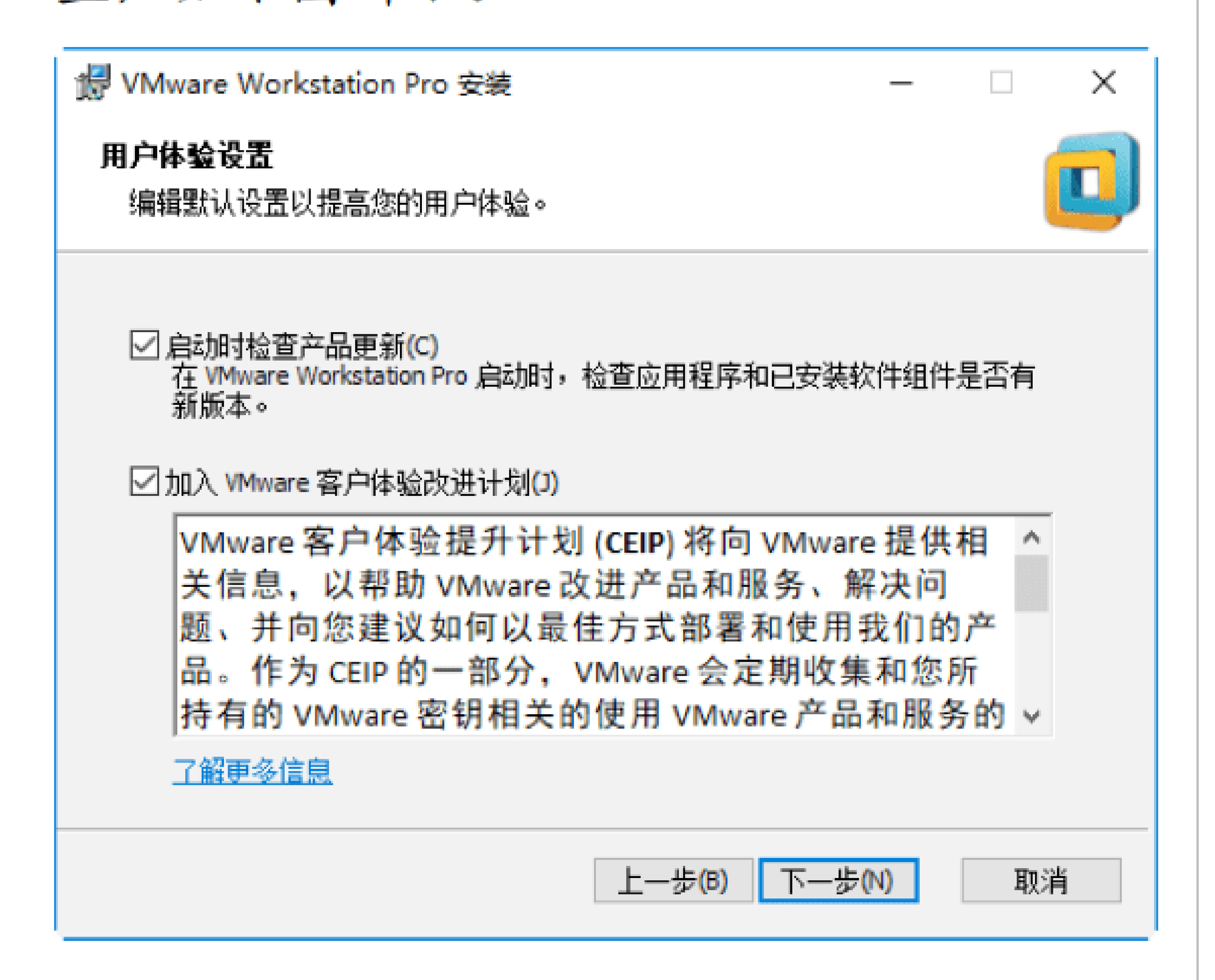


Step 03 单击“下一步”按钮，进入“自定义安装”对话框，在其中可以更改安装路径，也可以保持默认，如下图所示。

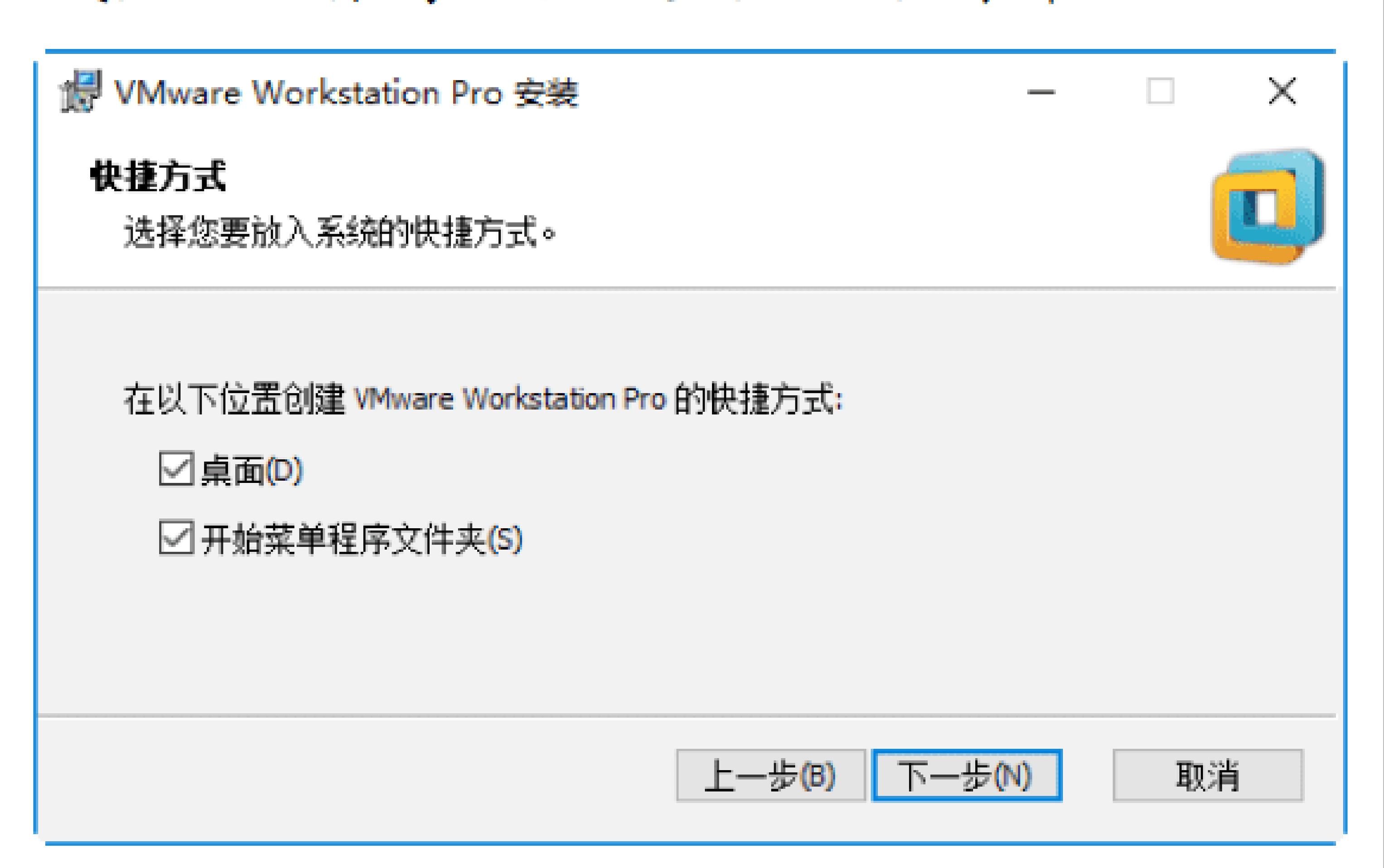




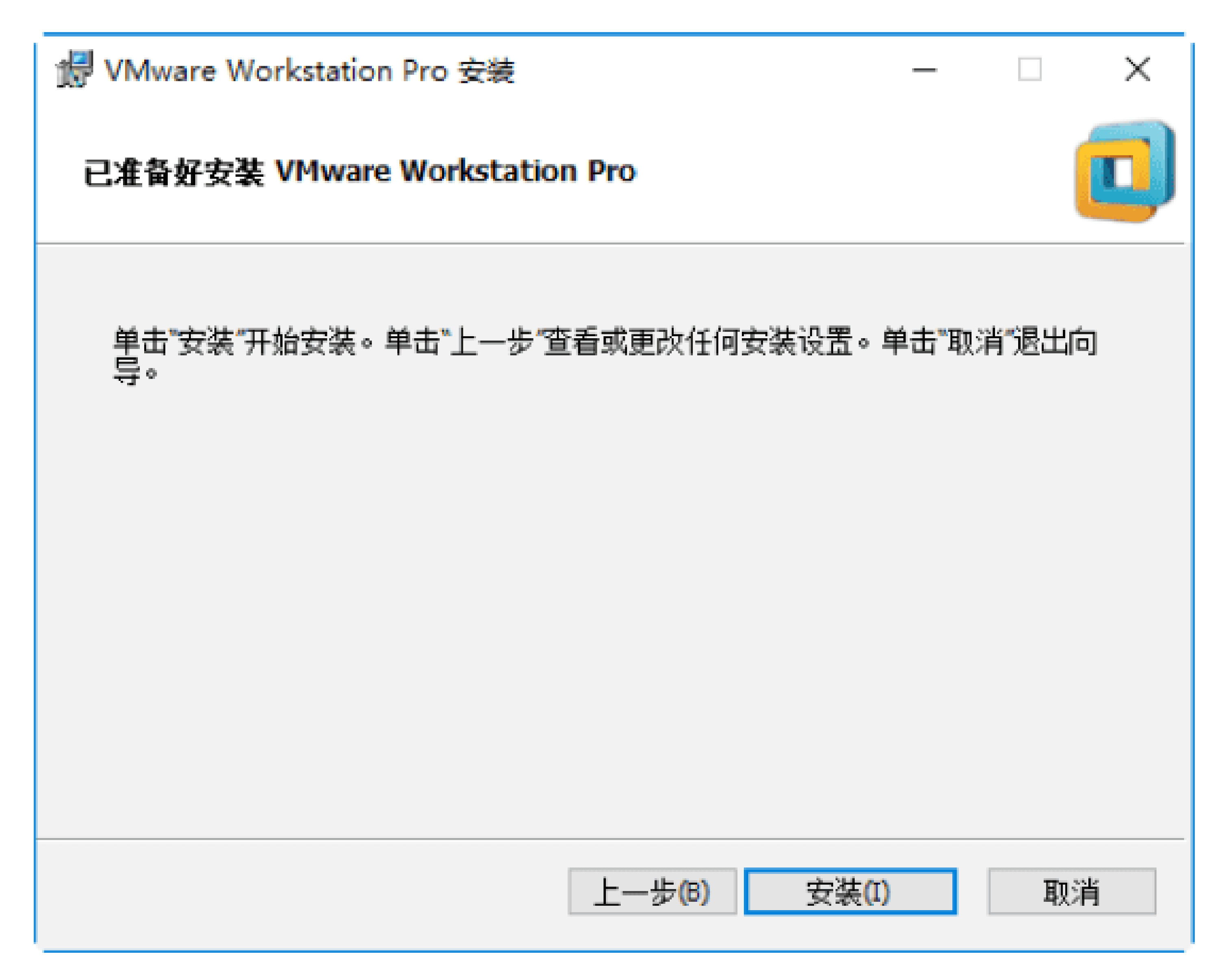
Step 04 单击“下一步”按钮，进入“用户体验设置”对话框，这里采用系统默认设置，如下图所示。



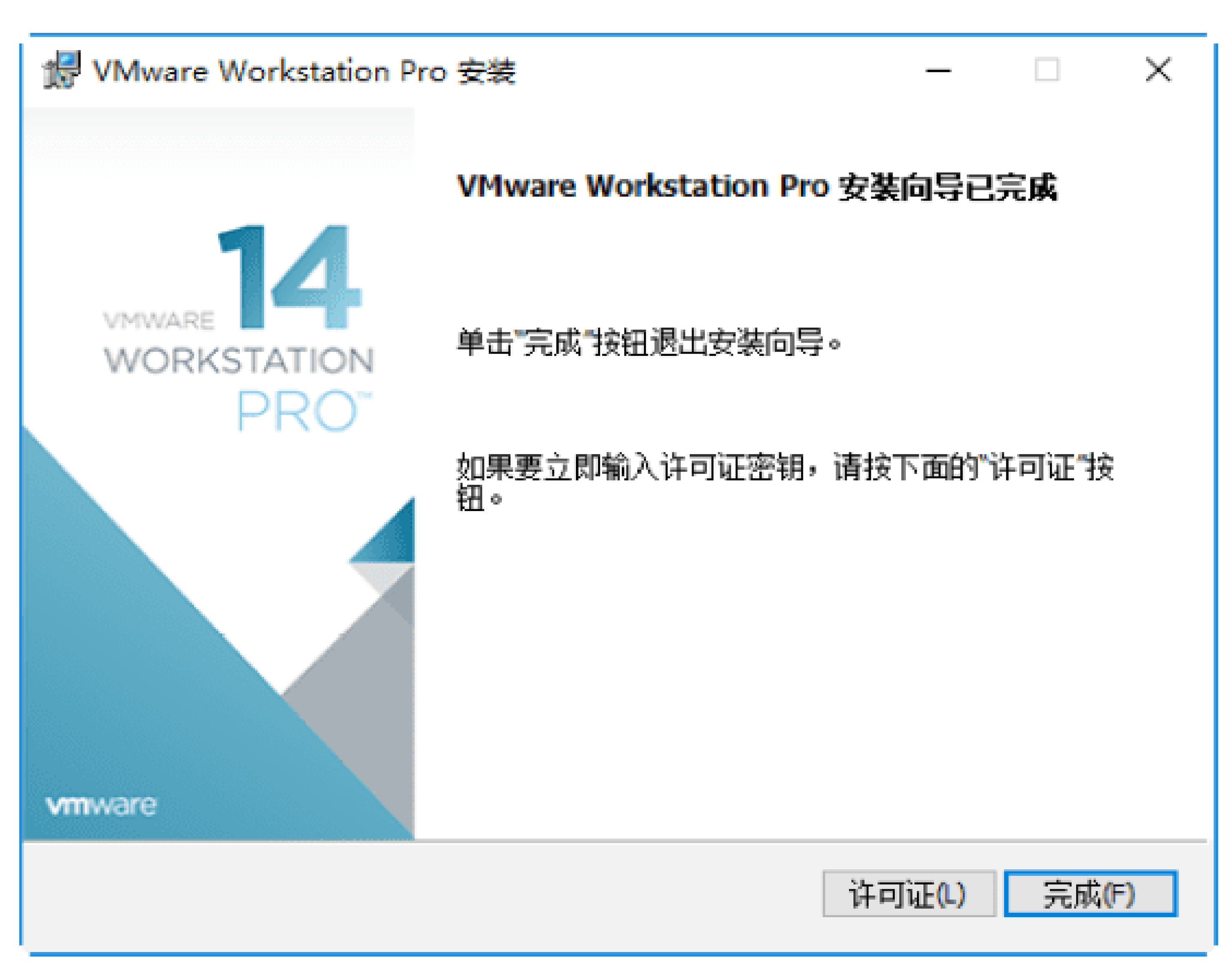
Step 05 单击“下一步”按钮，进入“快捷方式”对话框，在其中可以创建用户快捷方式，这里保持默认设置，如下图所示。



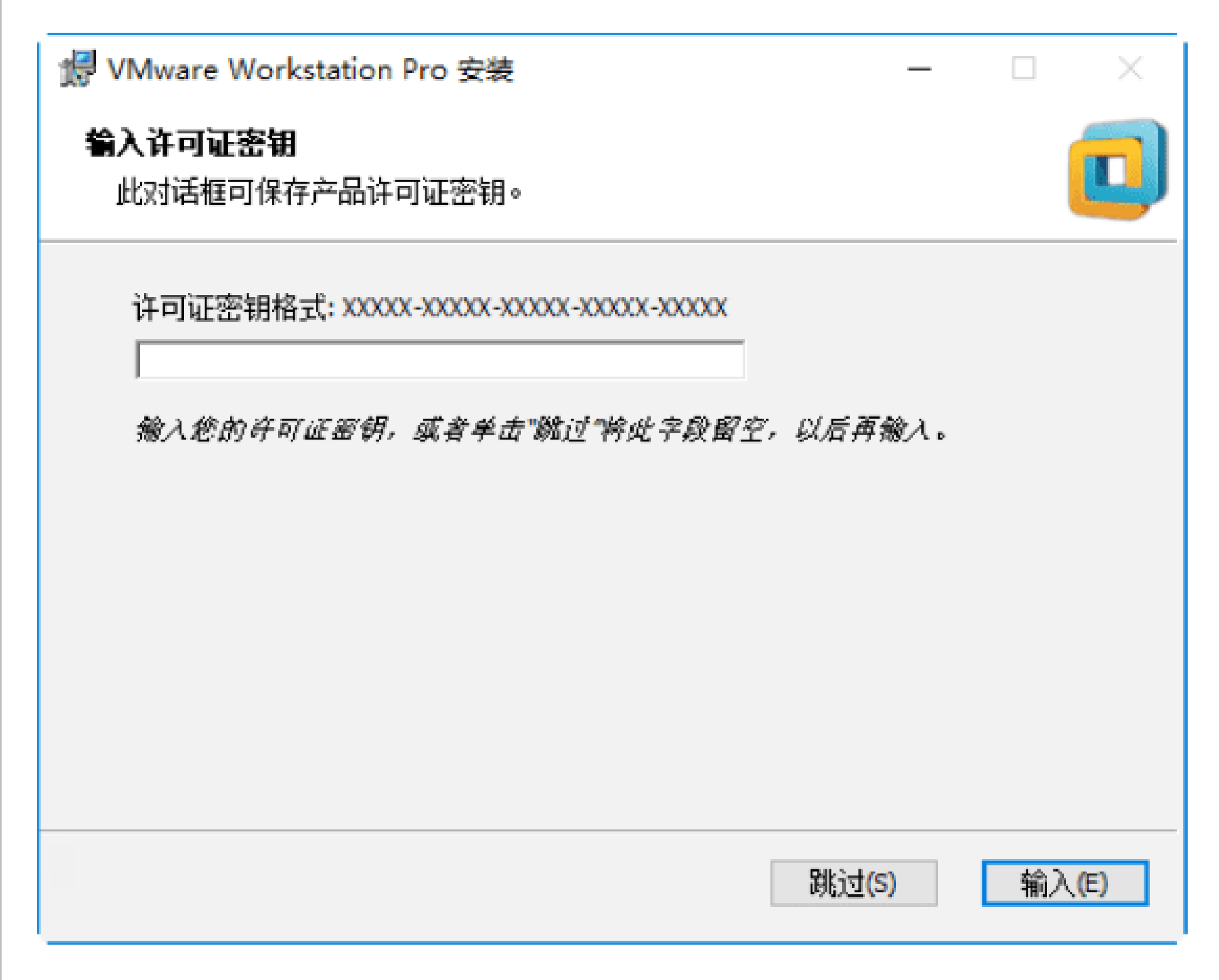
Step 06 单击“下一步”按钮，进入“已准备好安装VMware Workstation Pro”页面，开始准备安装虚拟机软件，如下图所示。



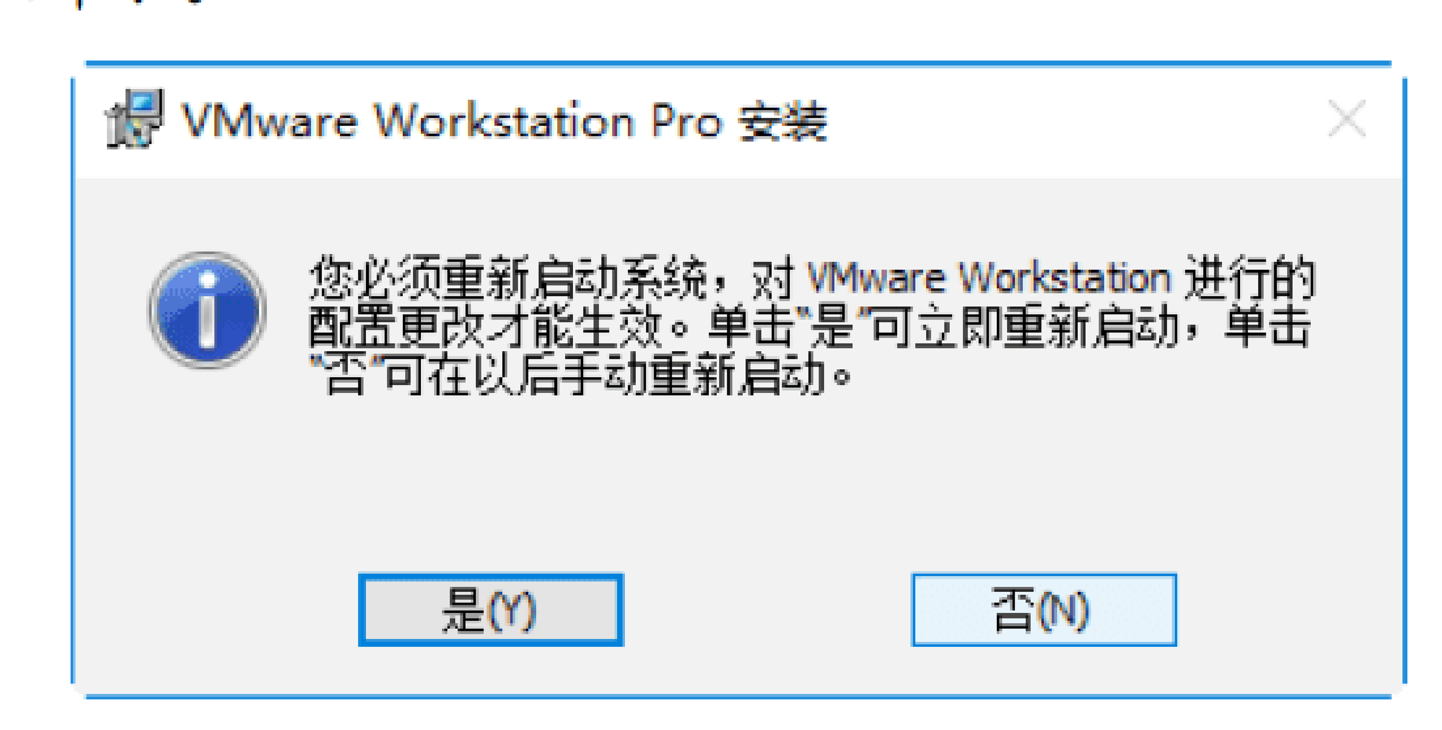
Step 07 单击“安装”按钮，等待一段时间后，虚拟机便可以安装完成，并进入“VMware Workstation Pro安装向导已完成”对话框，单击“完成”按钮，关闭虚拟机安装向导，如下图所示。



Step 08 在安装完成页面中，单击“许可证”按钮，跳转至“输入许可证密钥”页面，在其中可以输入许可证密钥，如下图所示。



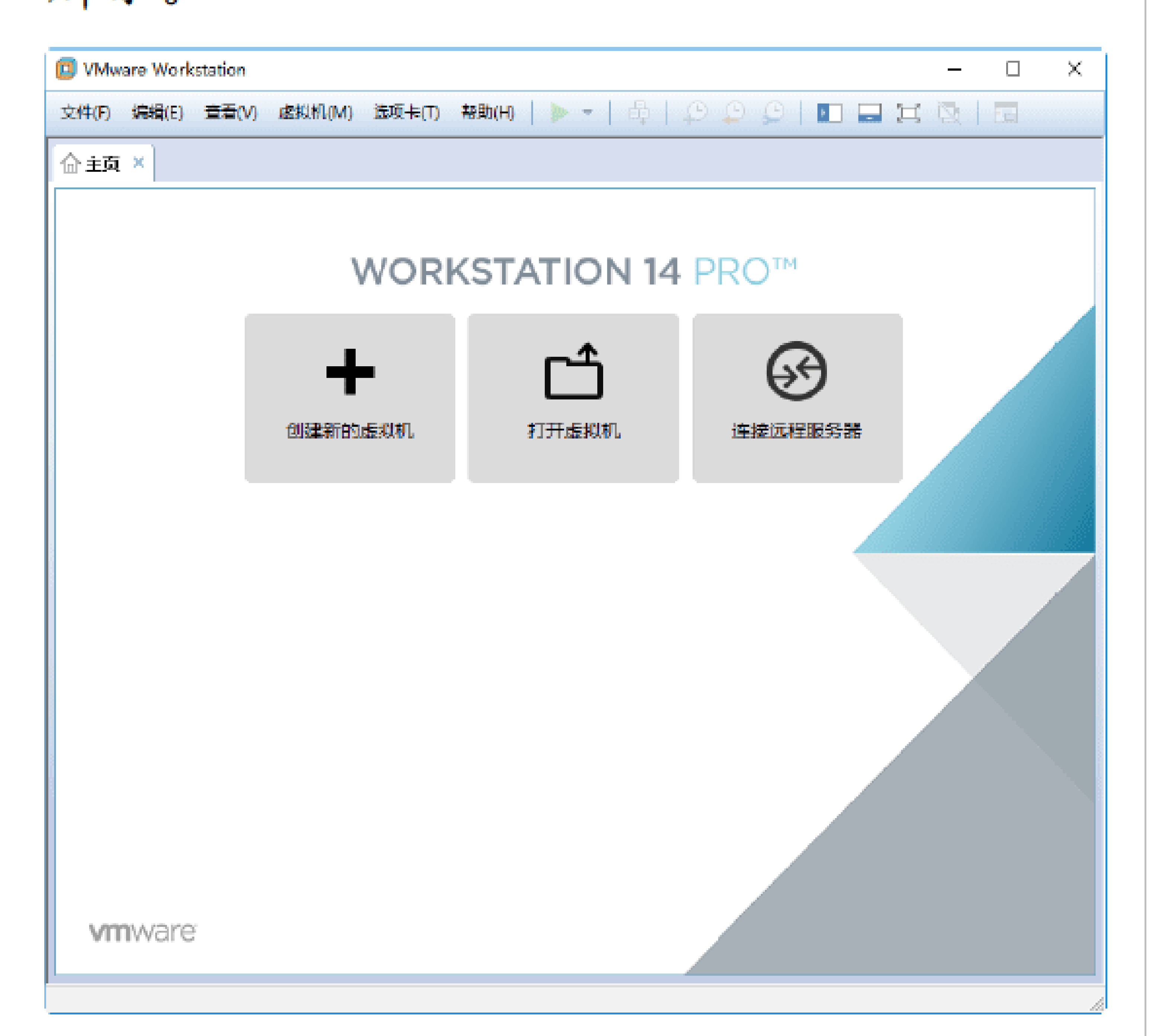
Step 09 虚拟机安装完成后，重新启动系统，才可以使用虚拟机，至此，便完成了VMware虚拟机的下载与安装，如下图所示。



实战3：创建虚拟机系统

虚拟机安装完成后，就需要创建一台真正的虚拟机，为后续的测试系统做准备。创建虚拟机的具体操作步骤如下。

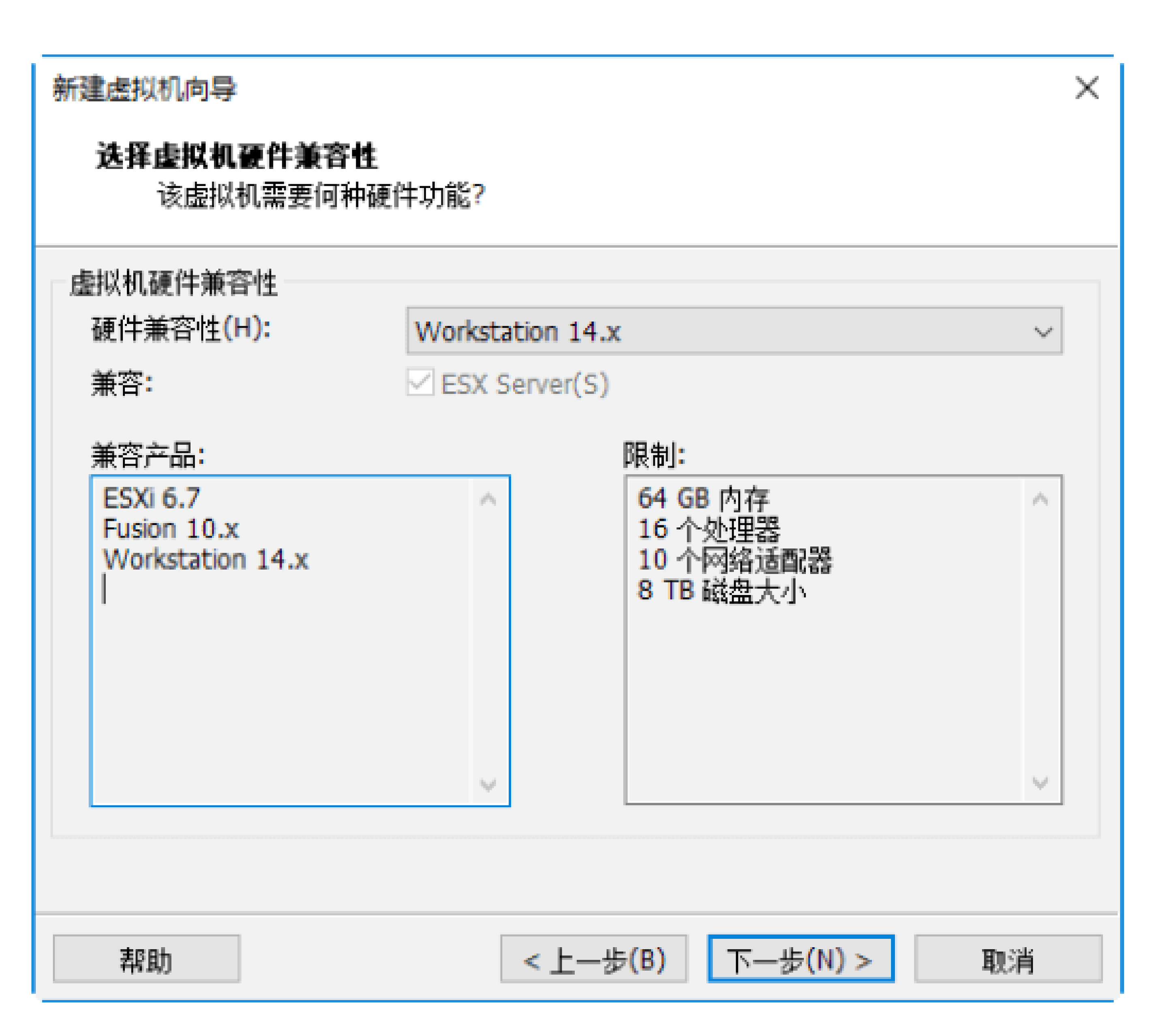
Step 01 双击桌面安装好的VMware虚拟机图标，打开VMware虚拟机软件，如下图所示。



Step 02 单击“创建新的虚拟机”按钮，进入“新建虚拟机向导”对话框，在其中选中“自定义”单选按钮，如下图所示。



Step 03 单击“下一步”按钮，进入“选择虚拟机硬件兼容性”对话框，在其中设置虚拟机的硬件兼容性，这里采用默认设置，如下图所示。

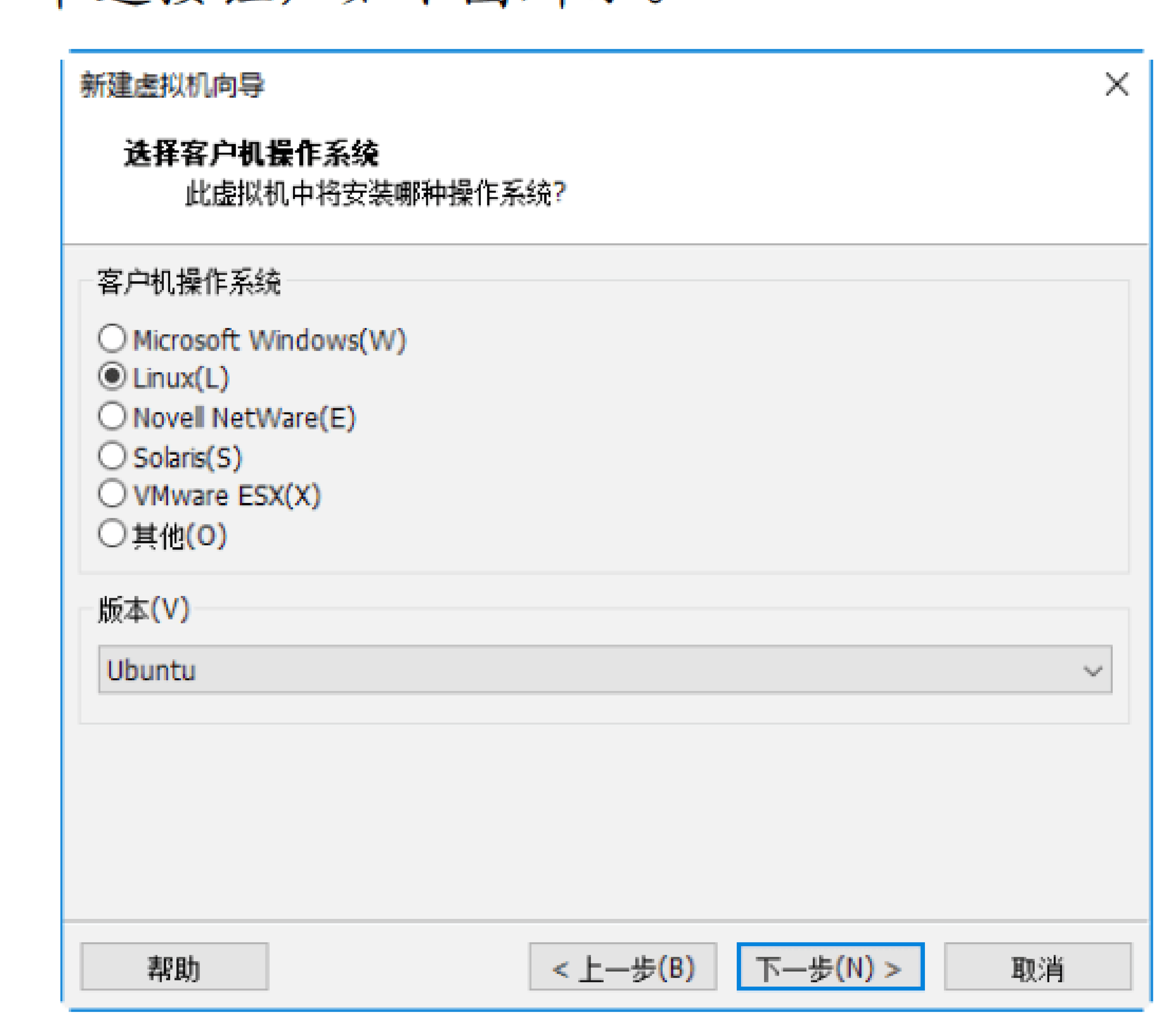




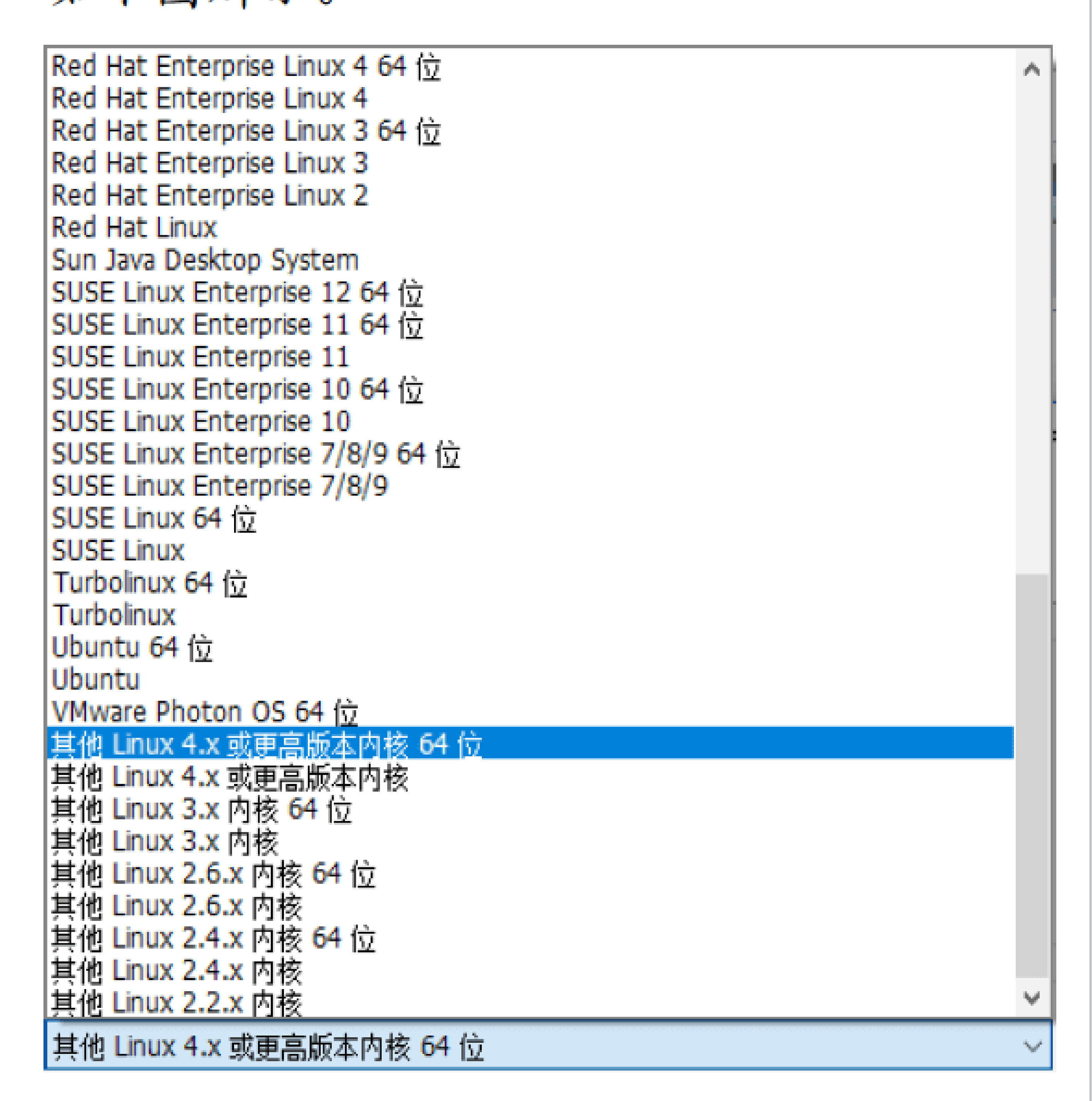
Step 04 单击“下一步”按钮，进入“安装客户机操作系统”对话框，在其中选中“稍后安装操作系统”单选按钮，如下图所示。



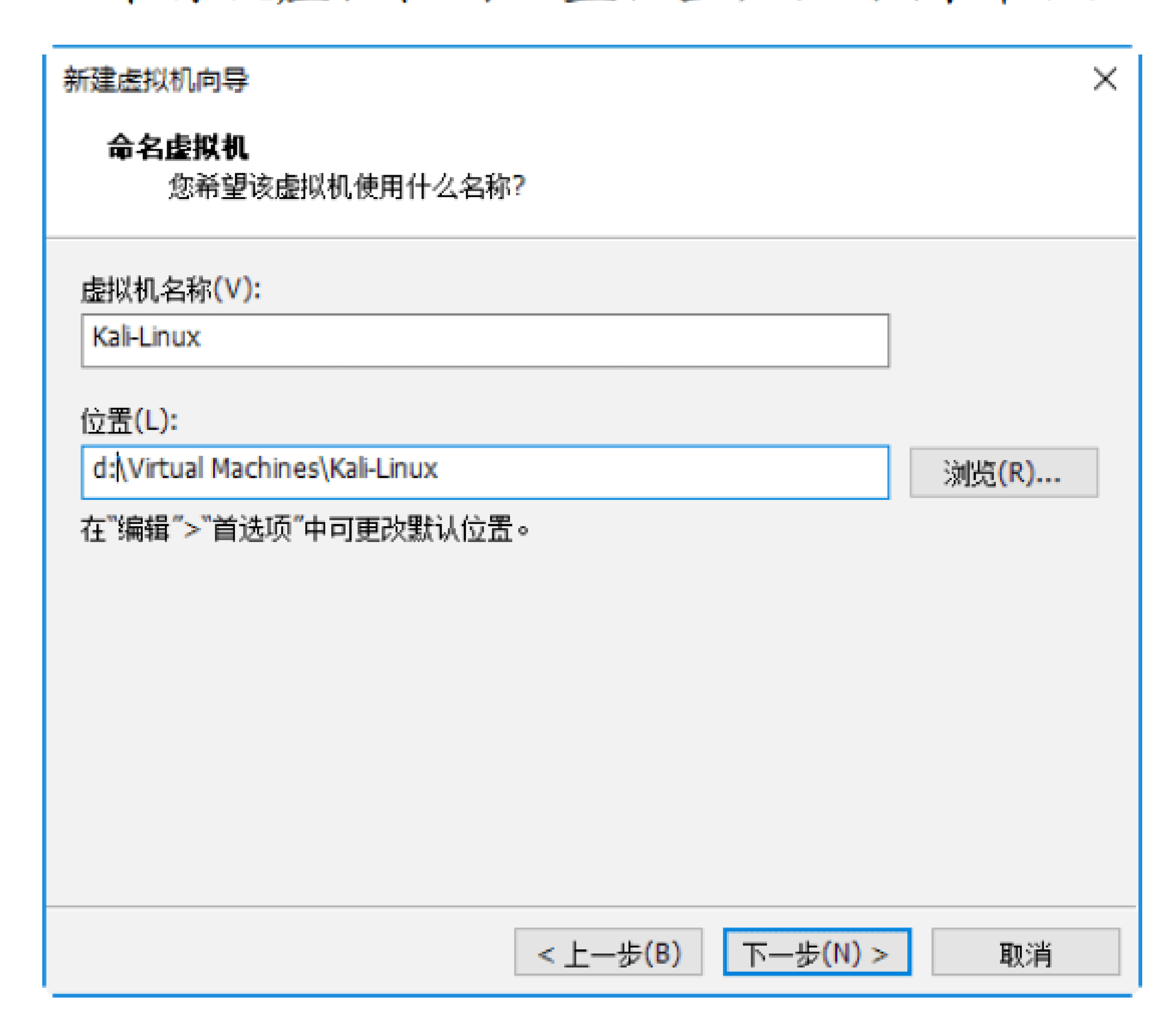
Step 05 单击“下一步”按钮，进入“选择客户机操作系统”对话框，在其中选中Linux单选按钮，如下图所示。



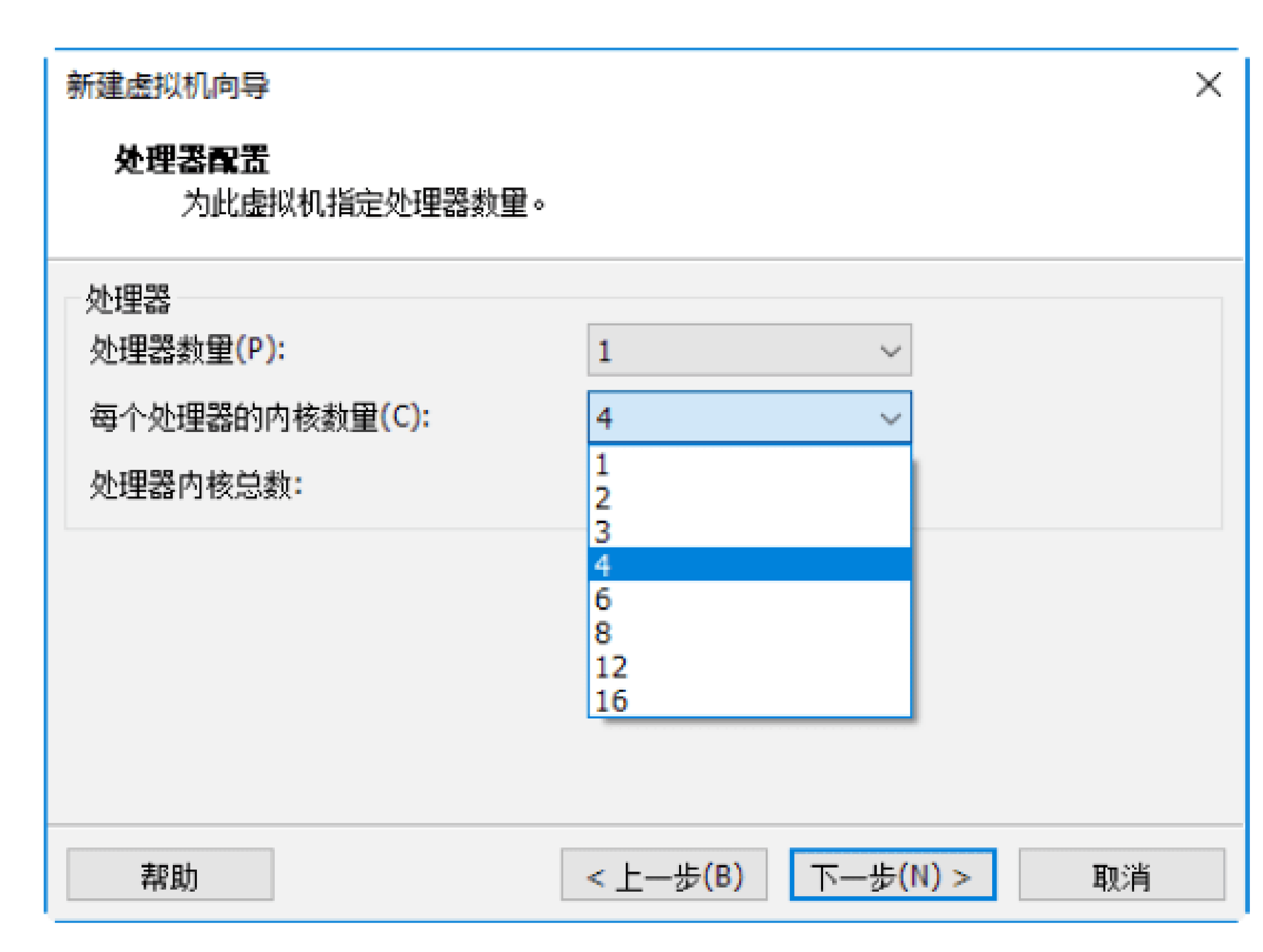
Step 06 单击“版本”下方的下拉按钮，在弹出的下拉列表中选择“其他Linux 4.x或更高版本内核64位”版本系统，这里的系统版本与主机系统版本无关，可以自由选择，如下图所示。



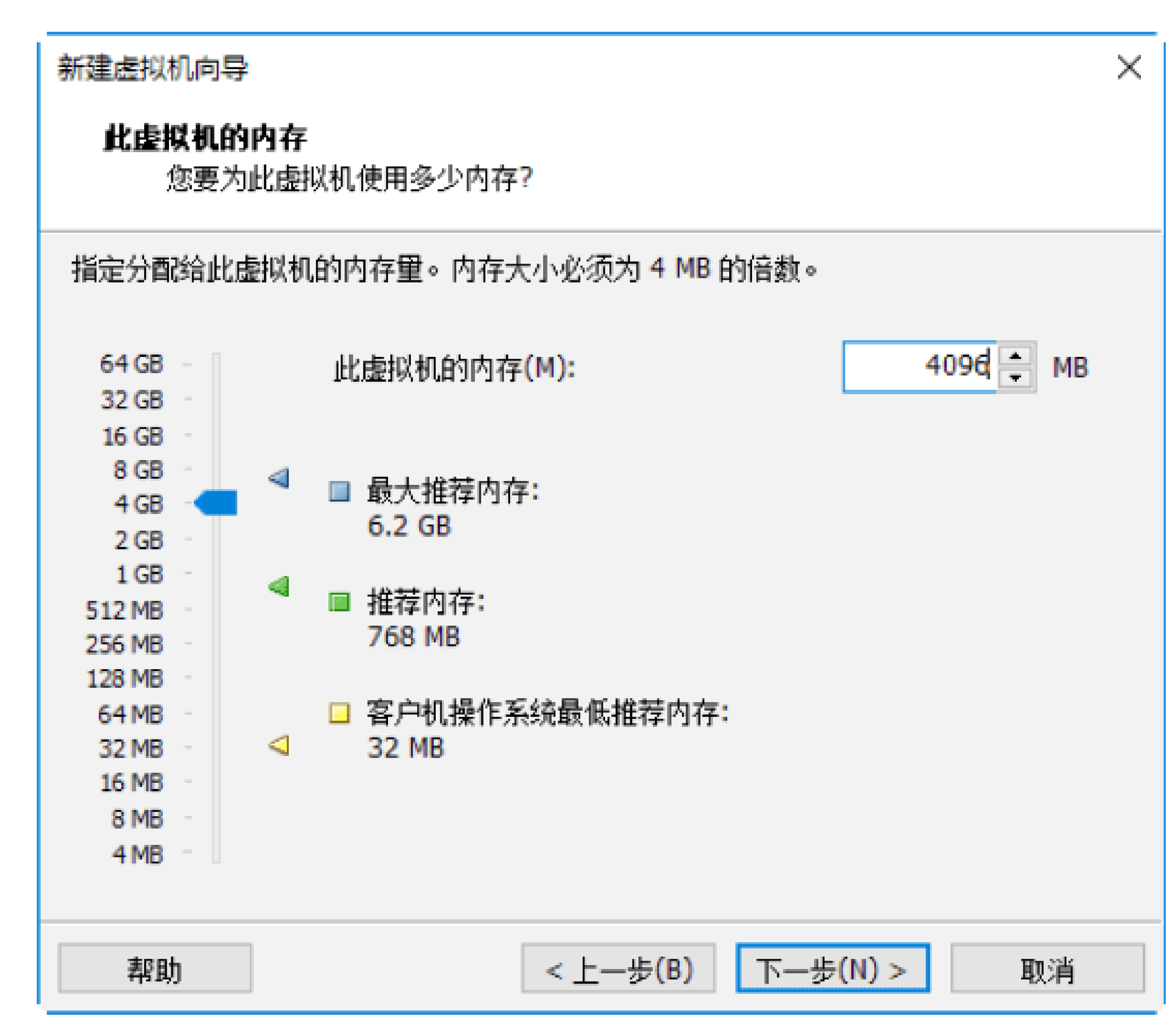
Step 07 单击“下一步”按钮，进入“命名虚拟机”对话框，在“虚拟机名称”文本框中输入虚拟机名称，在“位置”选项中选择一个存放虚拟机的磁盘位置，如下图所示。



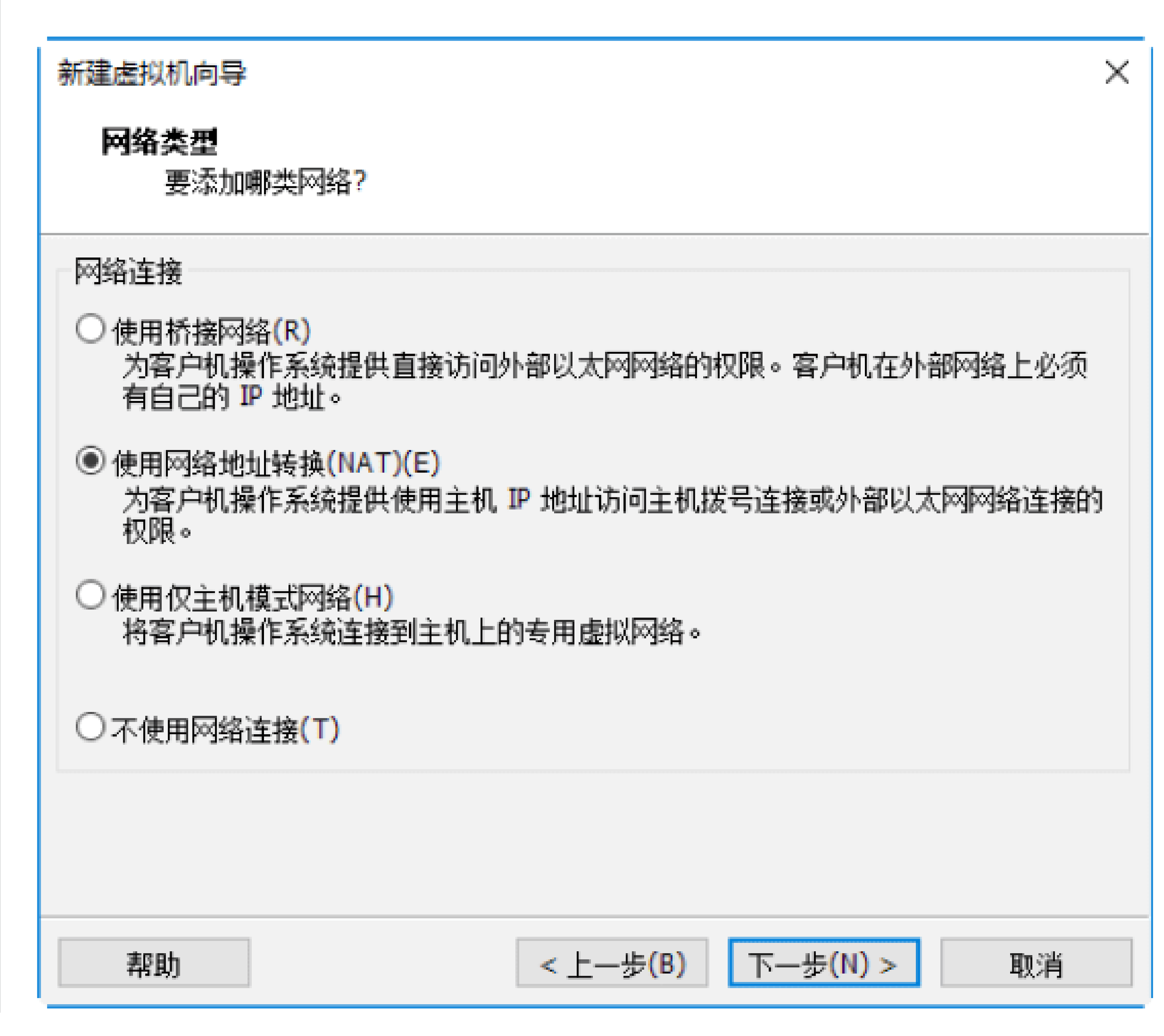
Step 08 单击“下一步”按钮，进入“处理器配置”对话框，在其中选择处理器数量。一般普通计算机都是单处理，所以这里不用设置，处理器内核数量可以根据实际处理器内核数量设置，如下图所示。



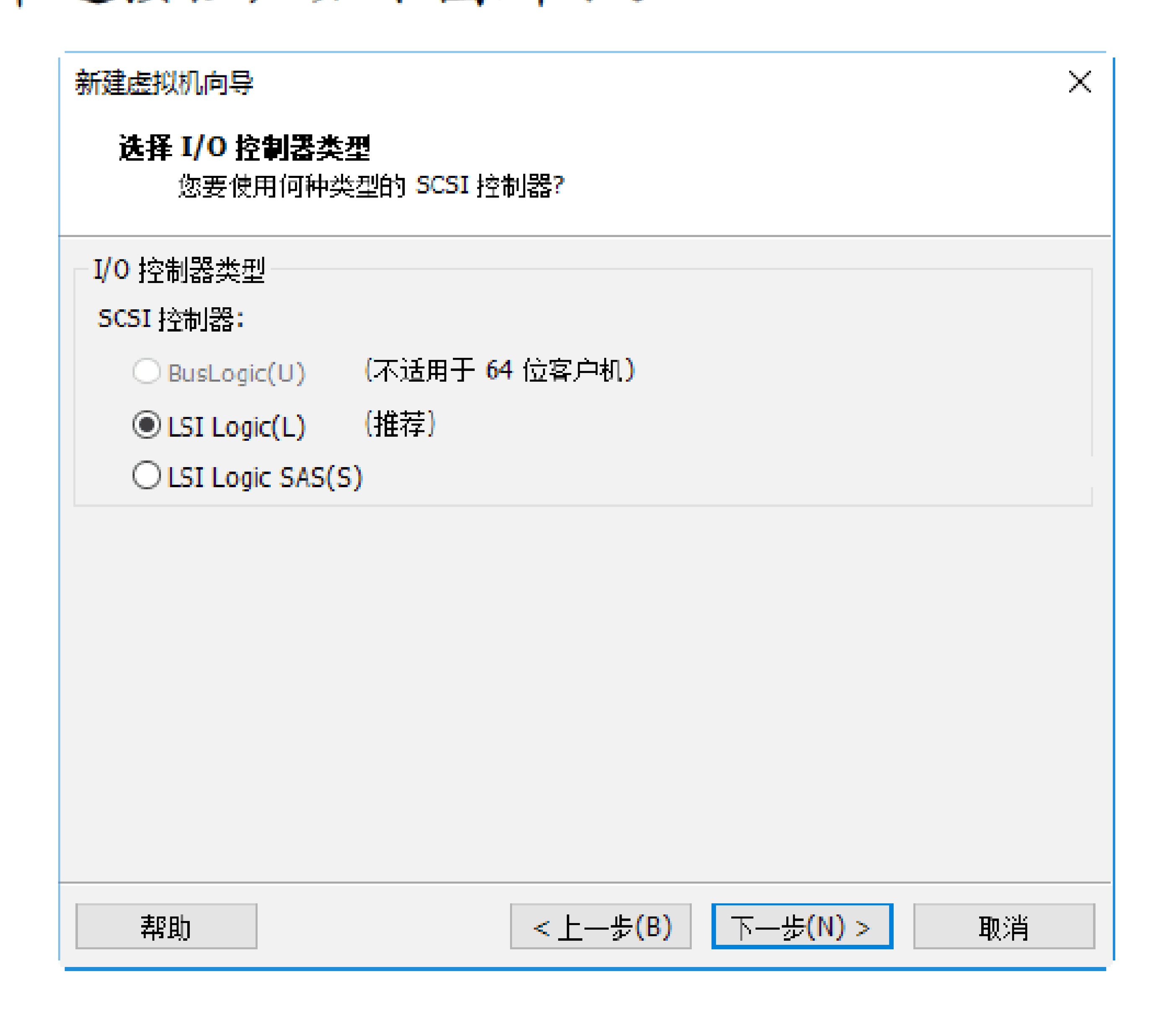
Step 09 单击“下一步”按钮，进入“此虚拟机的内存”对话框，根据实际主机进行设置，最少内存不要低于768MB，这里选择4096MB，也就是4G内存，如下图所示。



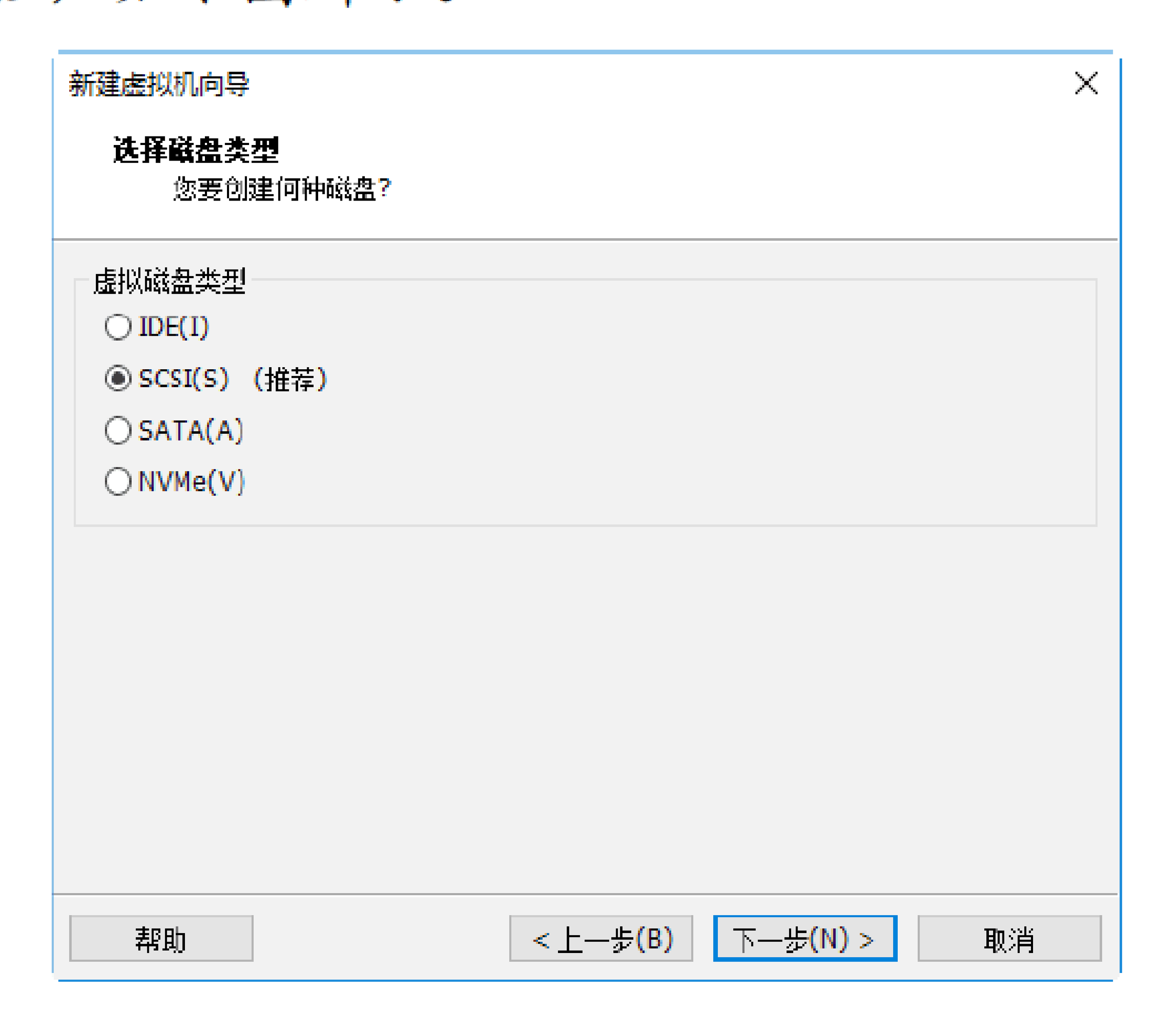
Step 10 单击“下一步”按钮，进入“网络类型”对话框，这里选中“使用网络地址转换（NAT）”单选按钮，如下图所示。



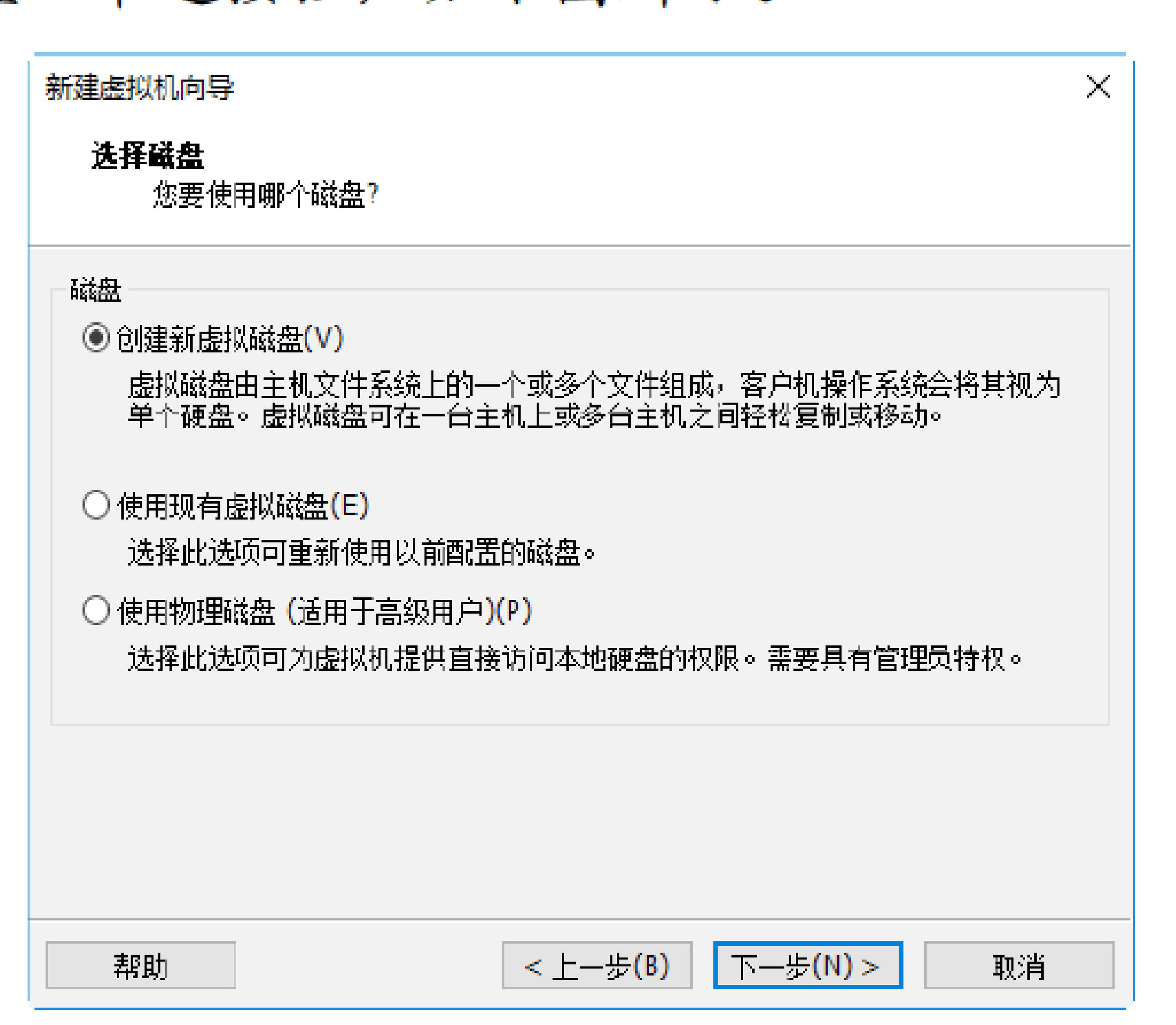
Step 11 单击“下一步”按钮，进入“选择I/O控制器类型”对话框，这里选中LSI Logic单选按钮，如下图所示。



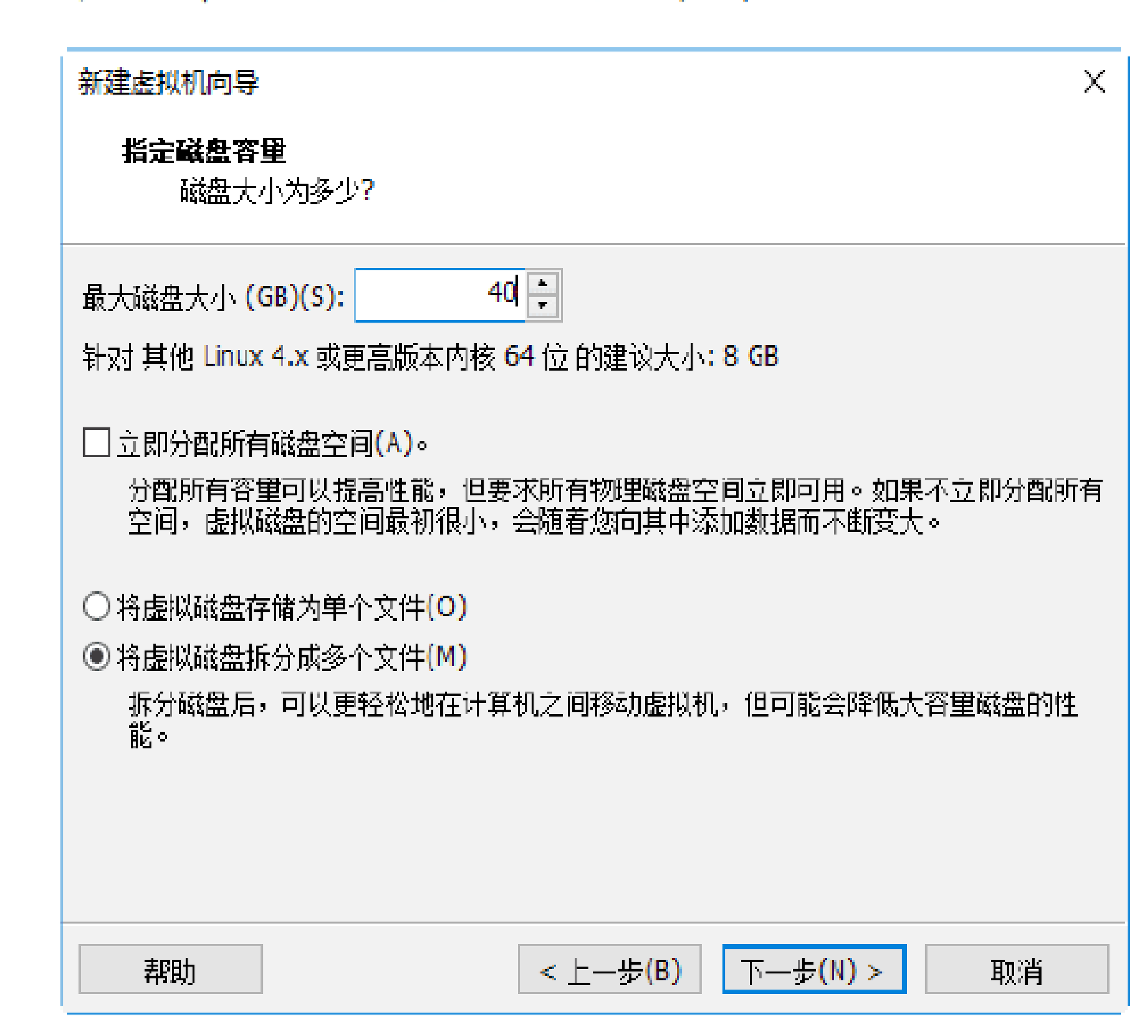
Step 12 单击“下一步”按钮，进入“选择磁盘类型”对话框，这里选中SCSI单选按钮，如下图所示。



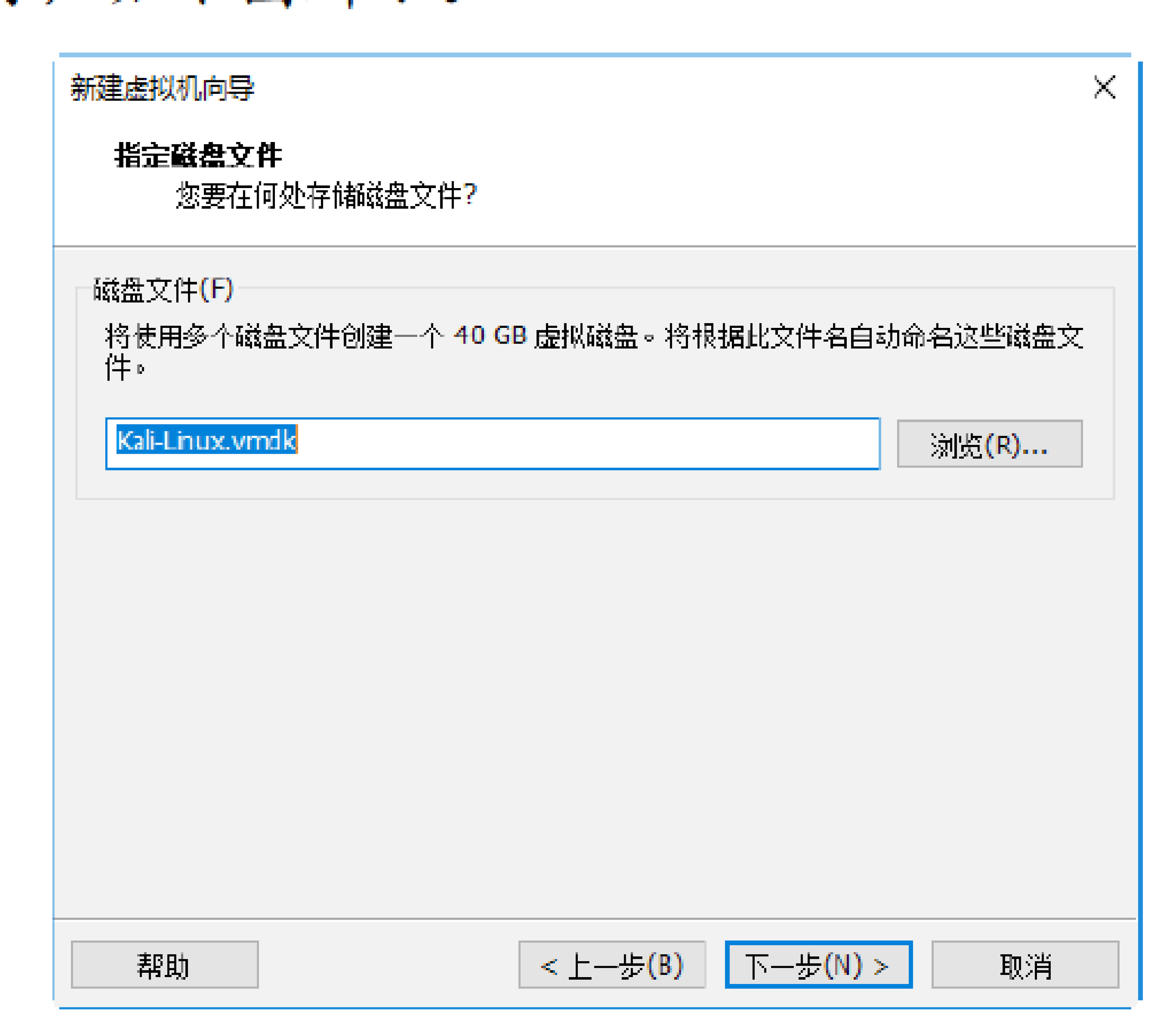
Step 13 单击“下一步”按钮，进入“选择磁盘”对话框，这里选中“创建新虚拟磁盘”单选按钮，如下图所示。



Step 14 单击“下一步”按钮，进入“指定磁盘容量”对话框，这里最大磁盘大小设置40GB即可，选中“将虚拟磁盘拆分成多个文件”单选按钮，如下图所示。



Step 15 单击“下一步”按钮，进入“指定磁盘文件”对话框，这里保持默认设置即可，如下图所示。



Step 16 单击“下一步”按钮，进入“已准备好创建虚拟机”对话框，如下图所示。

新建虚拟机向导

已准备好创建虚拟机

单击"完成"创建虚拟机。然后可以安装 其他 Linux 4.x 或更高版本内核 64 位。

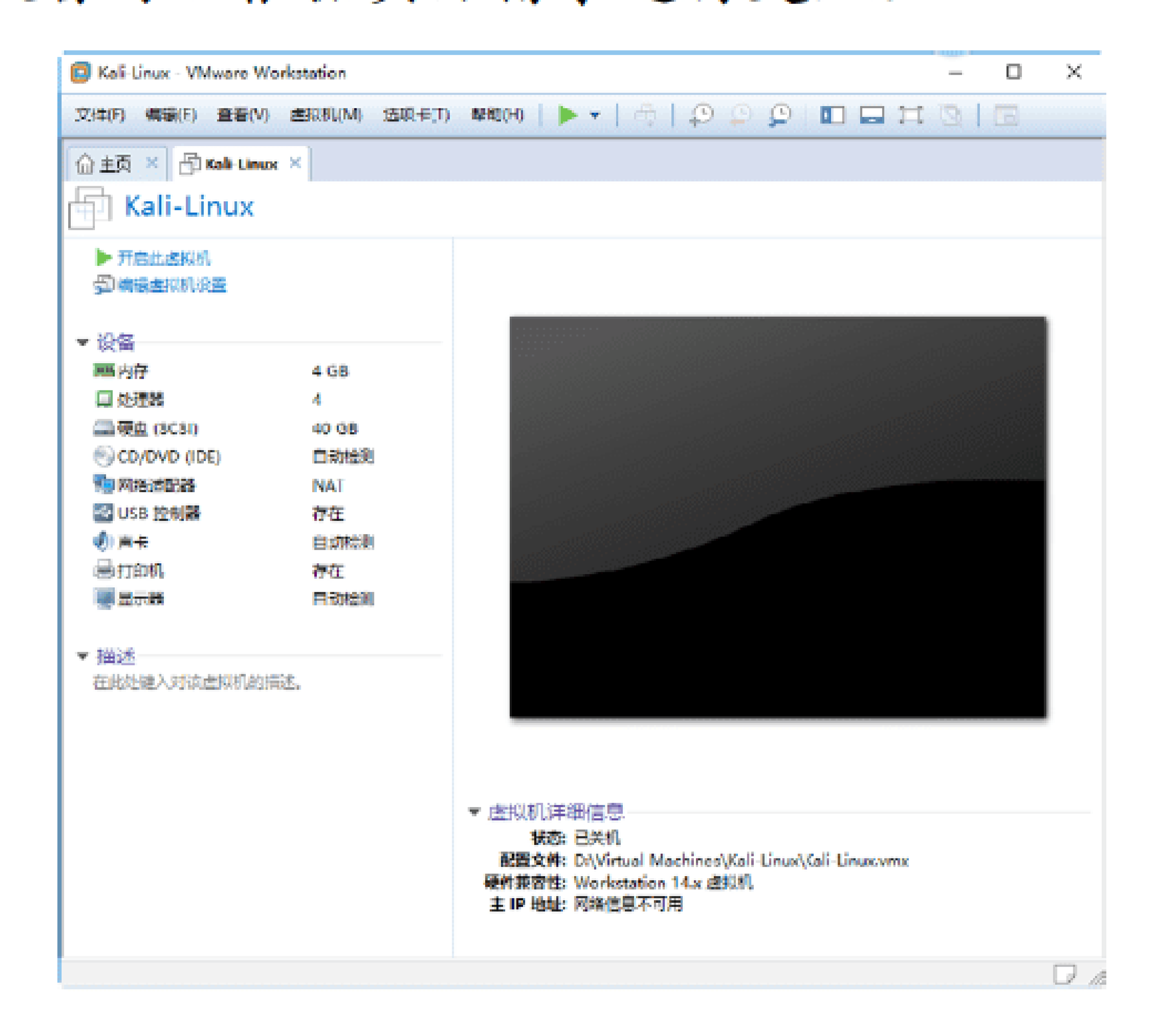
将使用下列设置创建虚拟机：

名称:	Kali-Linux
位置:	d:\Virtual Machines\Kali-Linux
版本:	Workstation 14.x
操作系统:	其他 Linux 4.x 或更高版本内核 64 位
硬盘:	40 GB, 拆分
内存:	4096 MB
网络适配器:	NAT
其他设备:	4 个 CPU 内核, CD/DVD, USB 控制器, 打印机, 声卡

自定义硬件(C)...

< 上一步(B)　完成　取消

Step 17 单击“完成”按钮，至此，便创建了一个新的虚拟机，如下图所示。这一步相当于组装了一台裸机计算机，其中的硬件设备可以根据实际需求进行更改。



2.3 安装虚拟机软件系统

现实中组装好计算机以后需要给它安装一个系统，这样计算机才可以正常工作。虚拟机也一样，同样需要安装一个操作系统，如Windows、Linux等，这样才能使用虚拟机创建的环境来实现网络安全测试。

实战4：安装Windows操作系统

在虚拟机中安装Windows操作系统是搭建网络安全测试环境的最重要步骤，所有准备工作就绪后，接下来就可以在虚拟机中安装Windows操作系统了。具体的操作步骤如下。

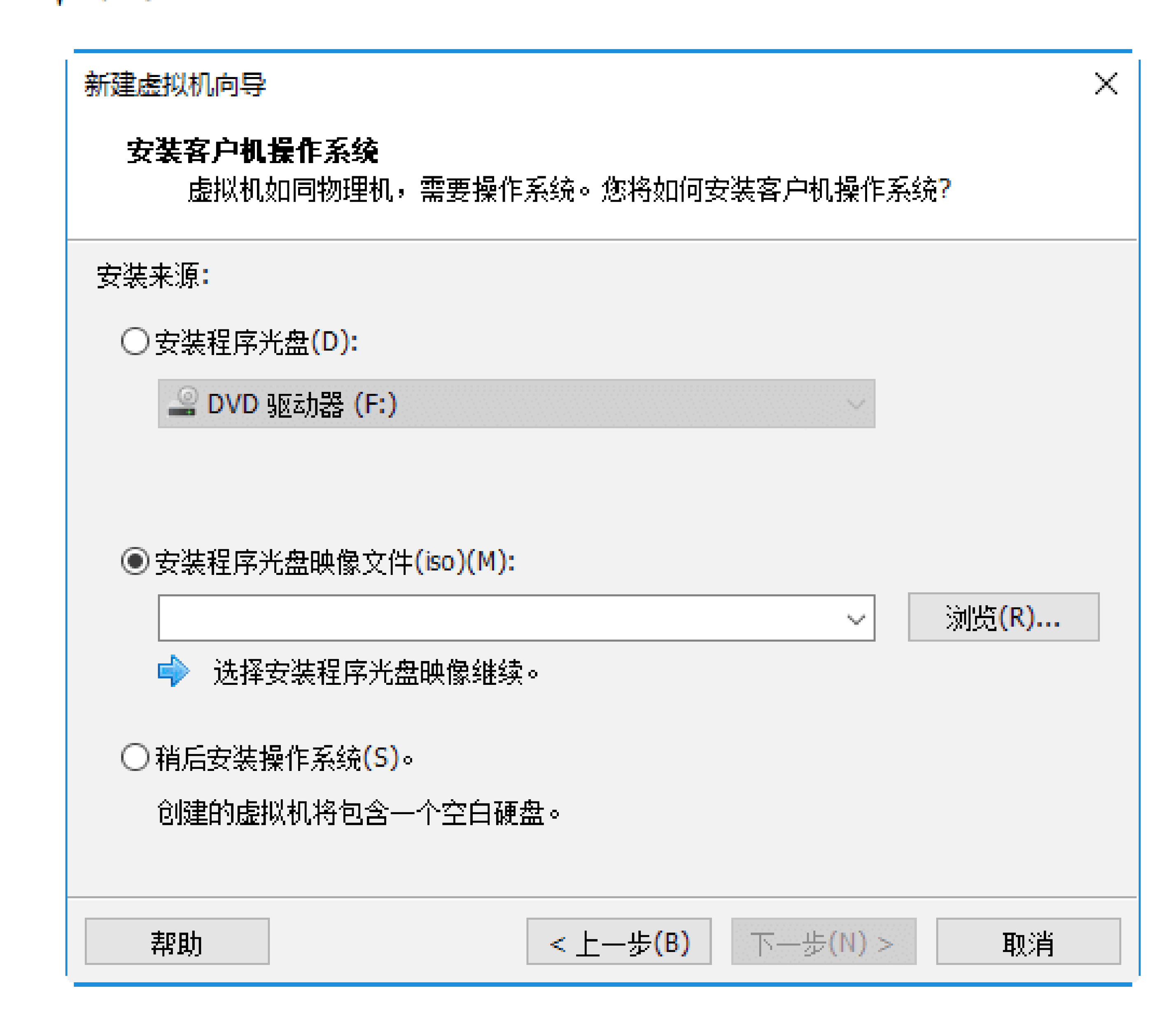
Step 01 在虚拟机的工作界面中单击“创建新的虚拟机”图标，如下图所示。



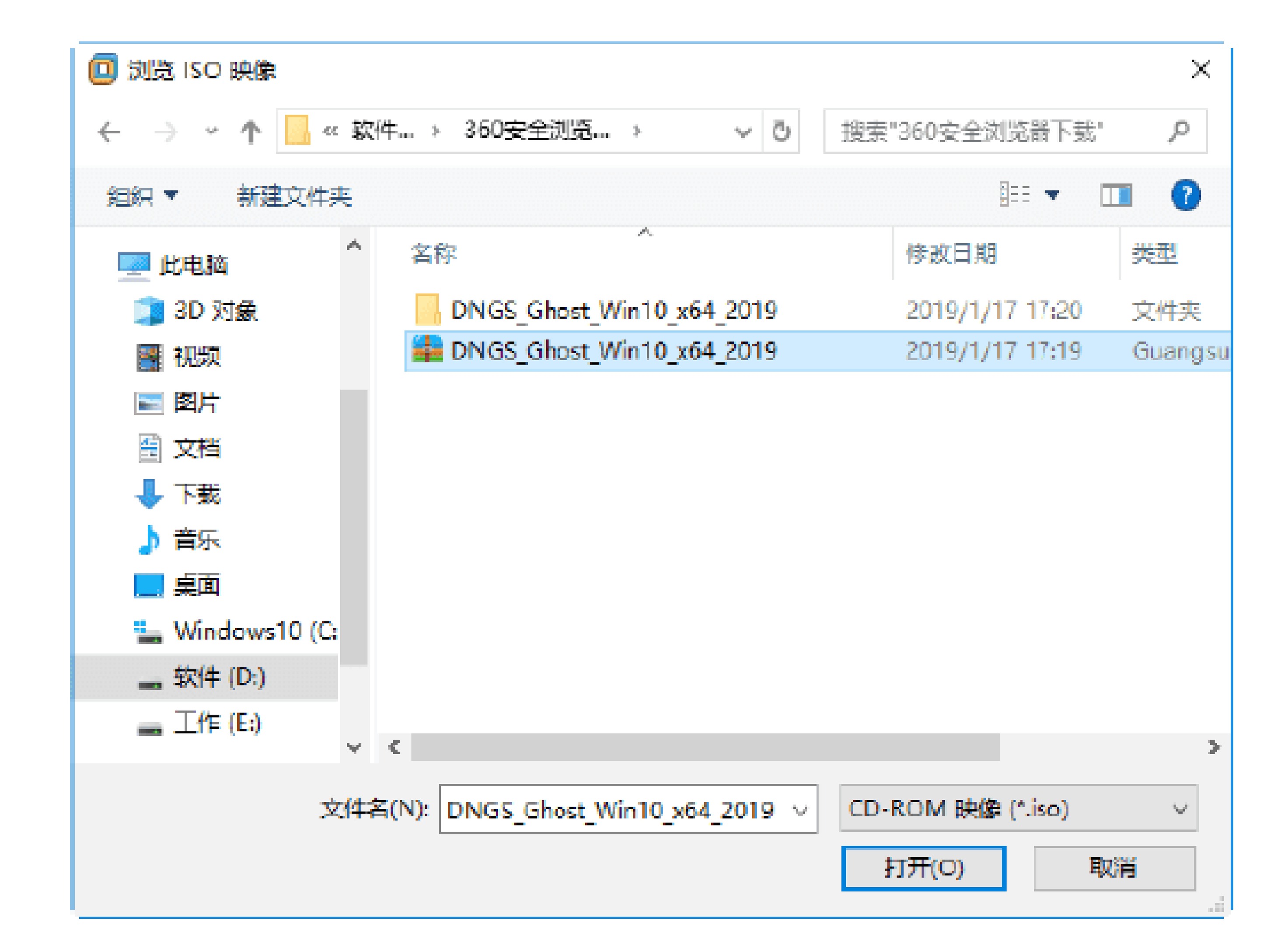
Step 02 弹出“欢迎使用新建虚拟机向导”对话框，在其中选中“典型（推荐）”单选按钮，如下图所示。



Step 03 单击“下一步”按钮，进入“安装客户机操作系统”对话框，在其中选中“安装程序光盘映像文件（iso）”单选按钮，如下图所示。



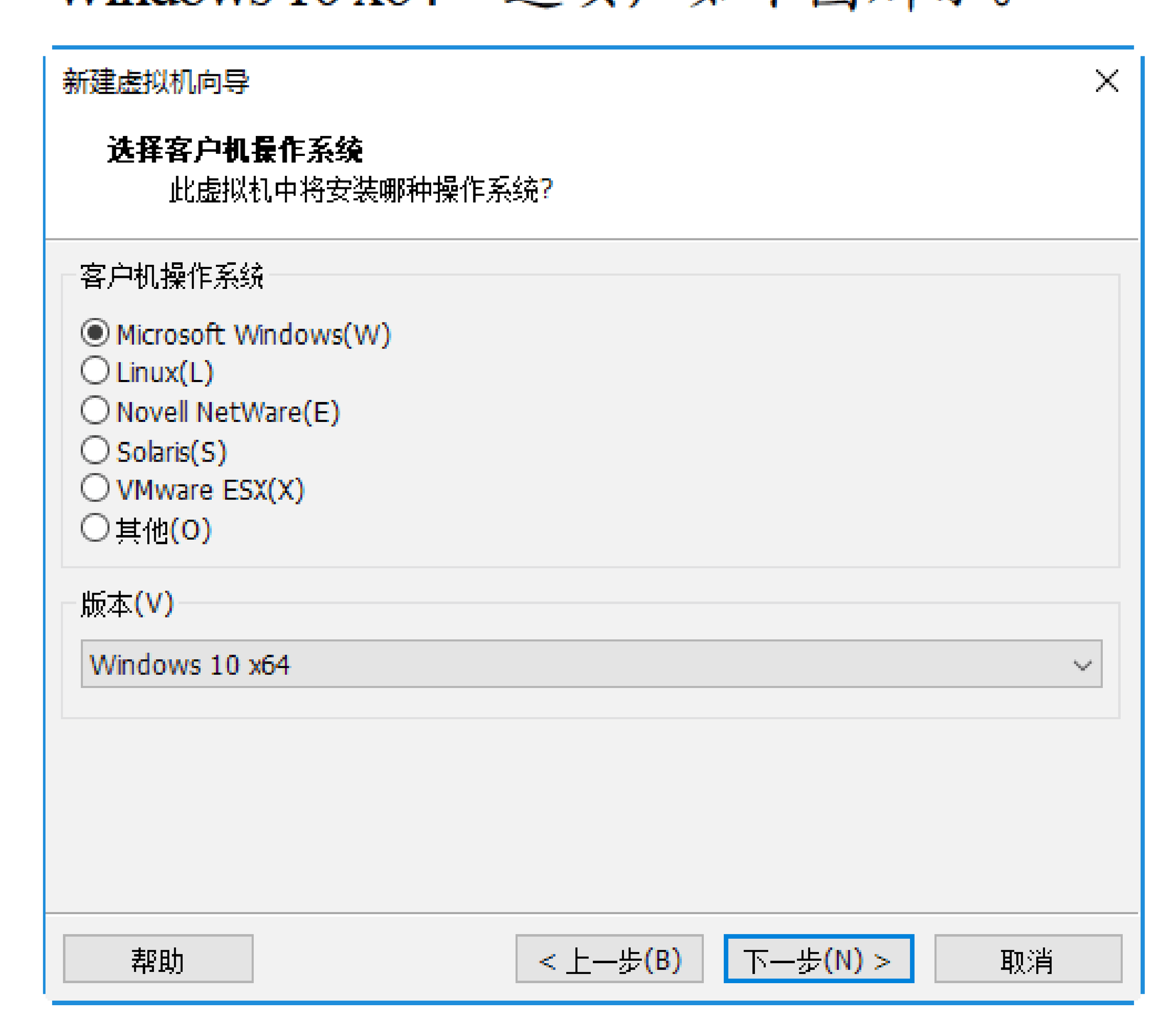
Step 04 单击“浏览”按钮，打开“浏览ISO映像”对话框，在其中选择需要安装的Windows操作系统，如下图所示。



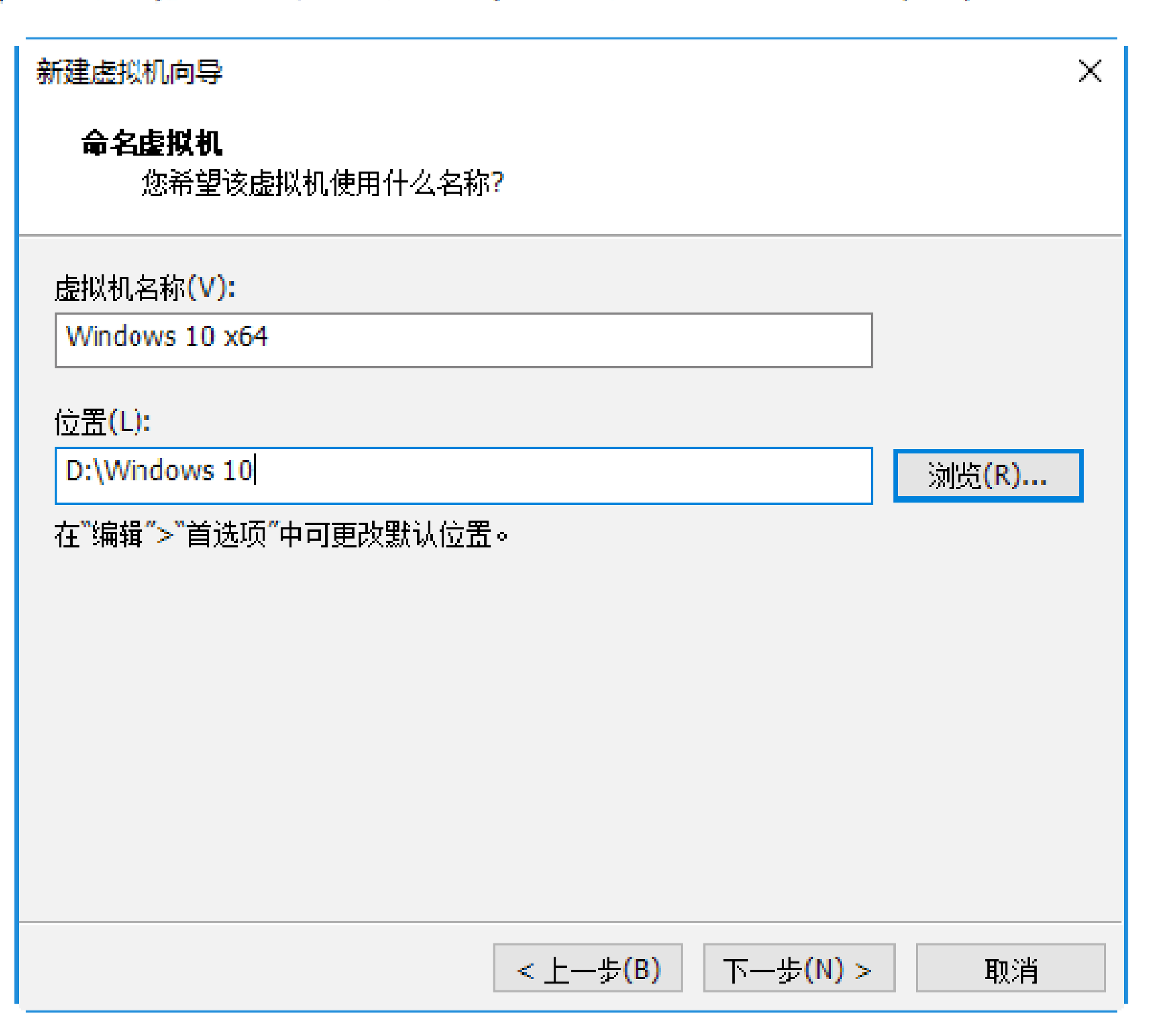
Step 05 单击“打开”按钮，返回到“安装客户机操作系统”对话框，如下图所示。



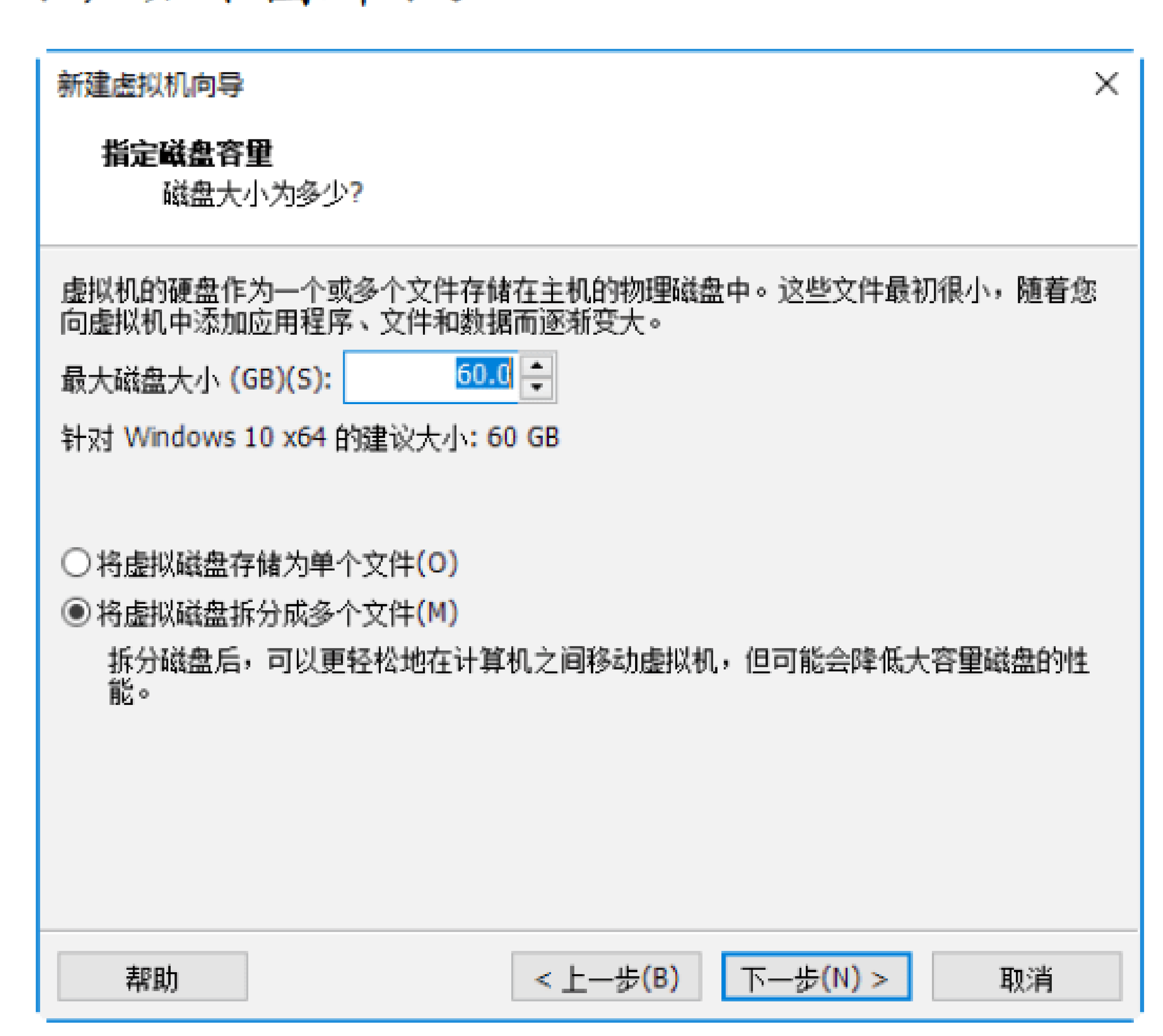
Step 06 单击“下一步”按钮，弹出“选择客户机操作系统”对话框，选中Microsoft Windows单选按钮，并在“版本”下拉列表中选择“Windows 10 x64”选项，如下图所示。



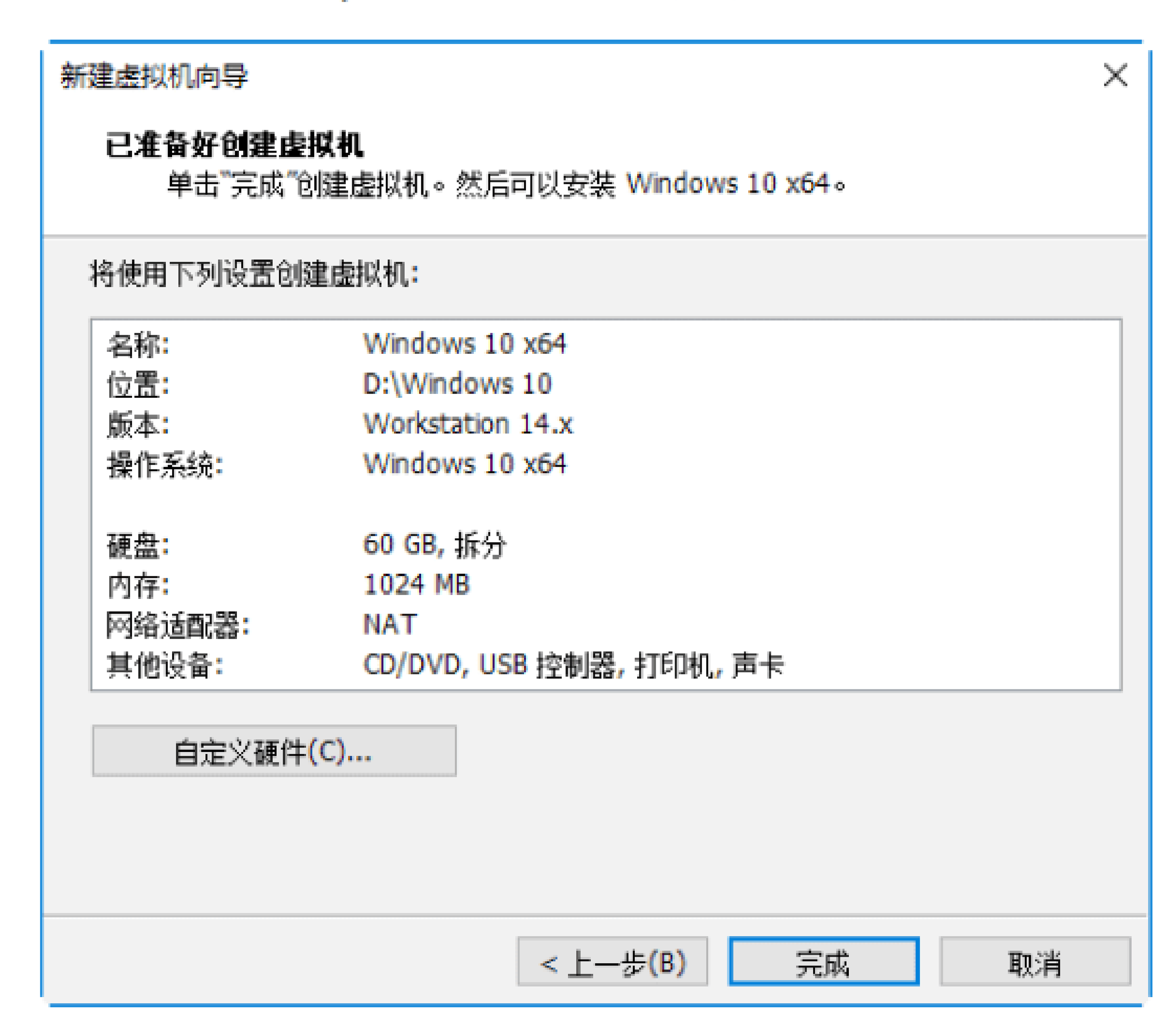
Step 07 单击“下一步”按钮，弹出“命名虚拟机”对话框，在其中输入虚拟机的名称，并设置虚拟机的安装位置，如下图所示。



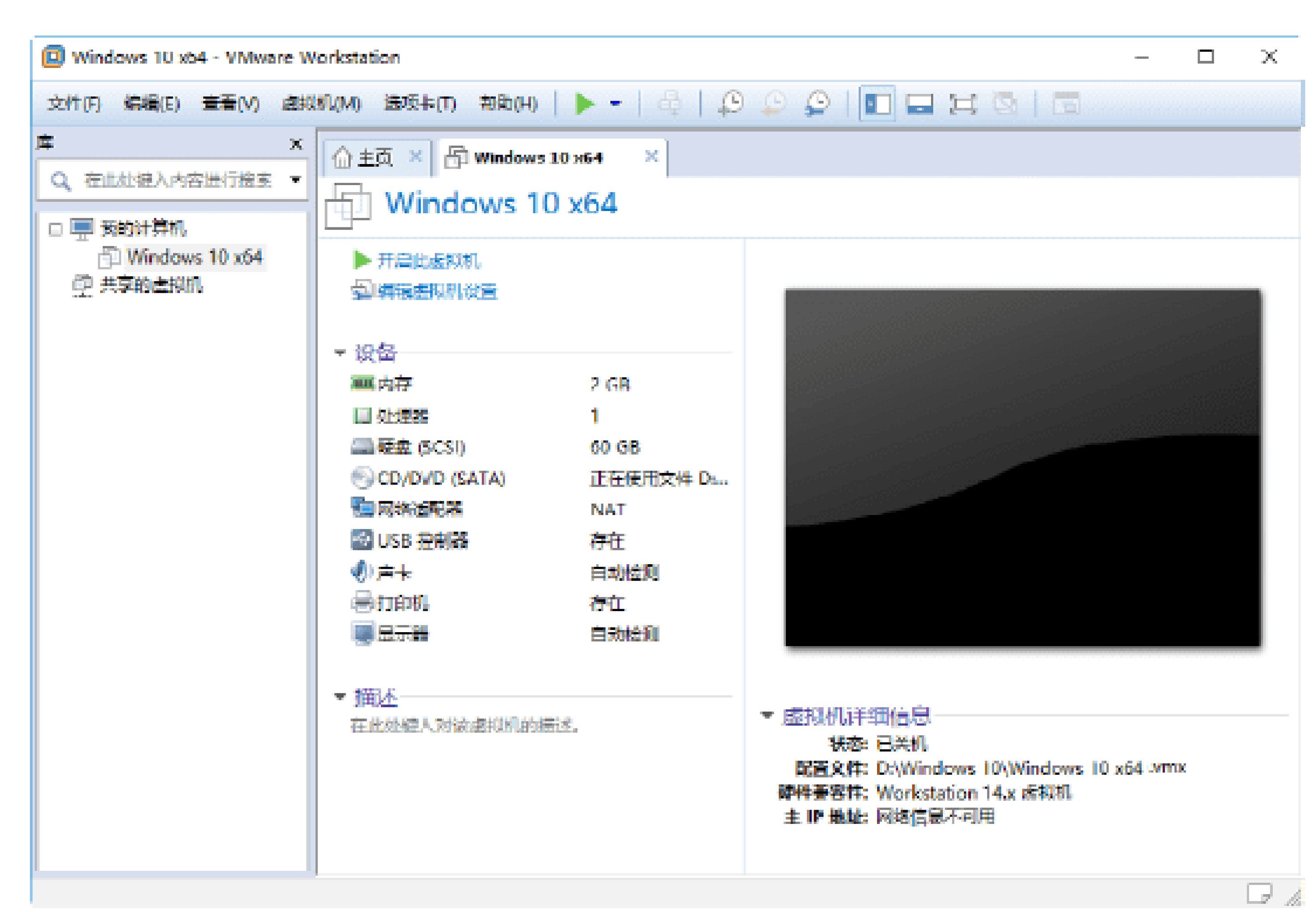
Step 08 单击“下一步”按钮，弹出“指定磁盘容量”对话框，在其中设置磁盘的大小，如下图所示。



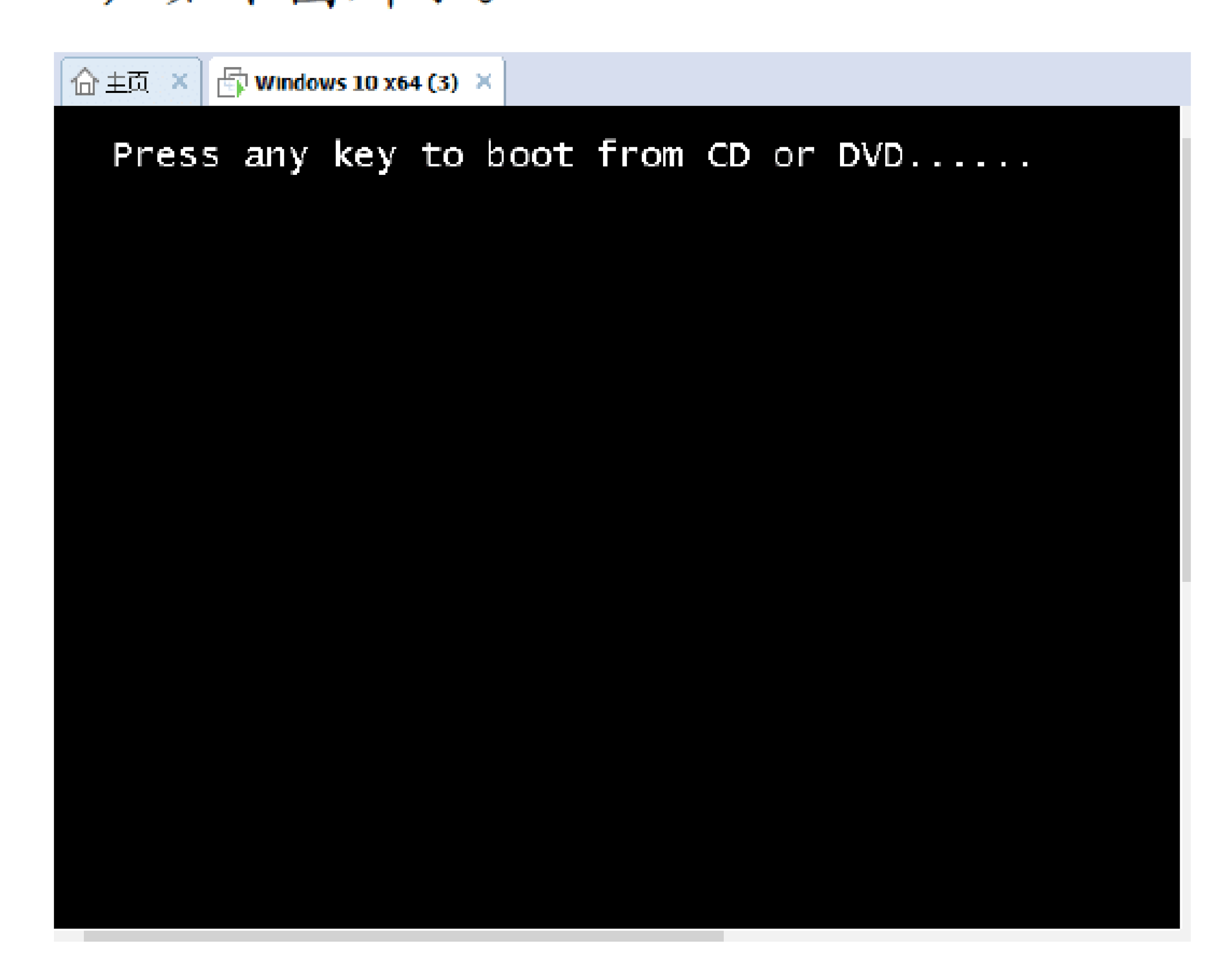
Step 09 单击“下一步”按钮，弹出“已准备好创建虚拟机”对话框，在其中显示了虚拟机的设置参数，如下图所示。



Step 10 单击“完成”按钮，进入虚拟机工作界面，如下图所示。



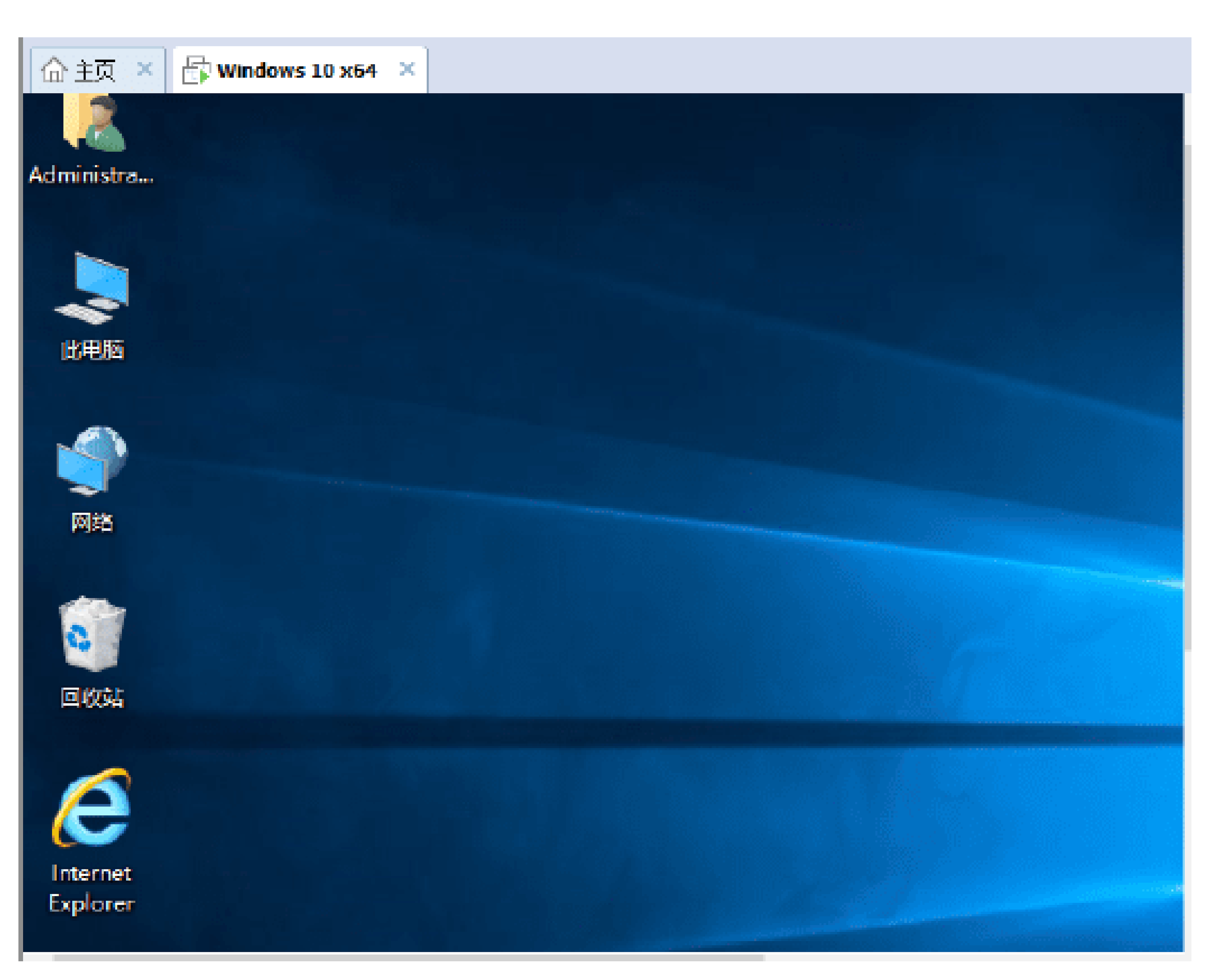
Step 11 单击“开启此虚拟机”链接，稍等片刻，Windows 10操作系统进入安装进程窗口，如下图所示。



Step 12 按任意键，即可打开“Windows安装程序”运行界面，安装程序将开始自动复制安装的文件并准备要安装的文件，如下图所示。



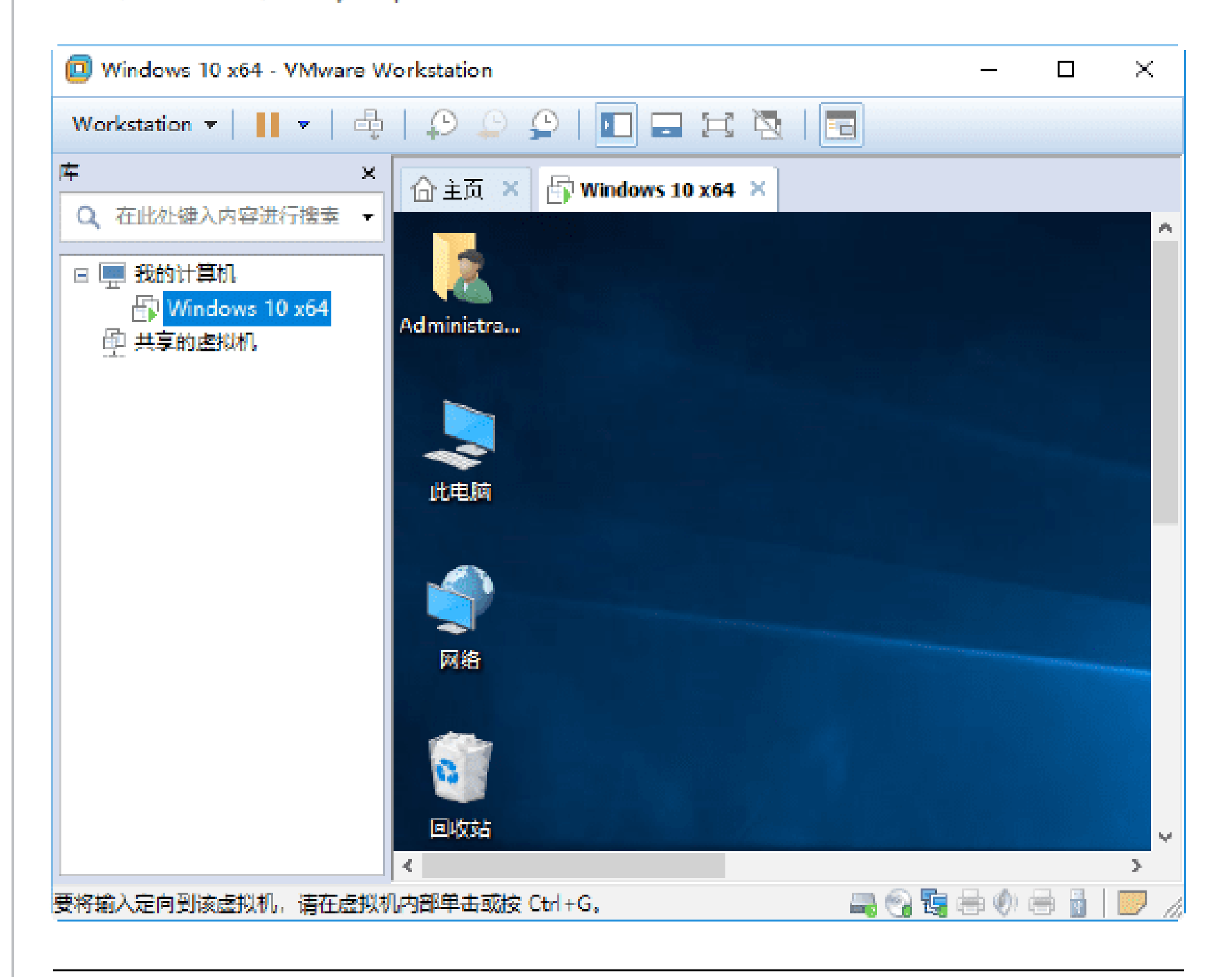
Step 13 安装完成后，将显示安装后的操作系统界面，如下图所示。至此，整个虚拟机的设置创建即可完成，安装的虚拟操作系统以文件的形式存放在硬盘中。



实战5：安装VMware Tools工具

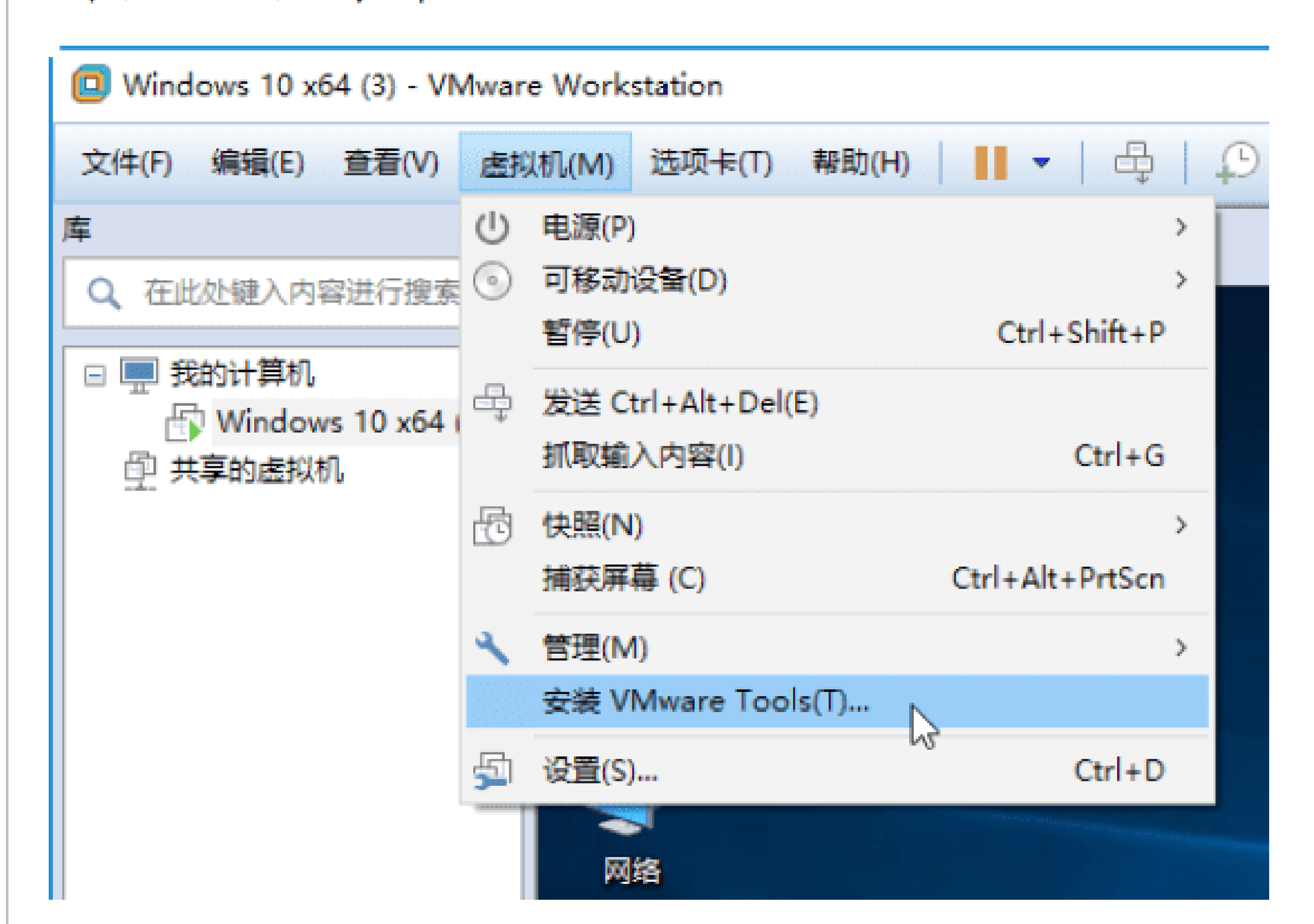
众所周知，本地计算机安装好操作系统之后，还需要安装各种驱动，如显卡、网卡、显卡等驱动，作为虚拟机也需要安装一定的虚拟工具才能正常运行。安装VMware Tools工具的操作步骤如下。

Step 01 启动虚拟机进入虚拟系统，然后按Ctrl+Alt组合键，切换到真实的计算机系统，如下图所示。



注意：如果是用ISO文件安装的操作系统，最好重新加载该安装文件并重新启动系统，这样系统就能自动找到VMware Tools的安装文件。

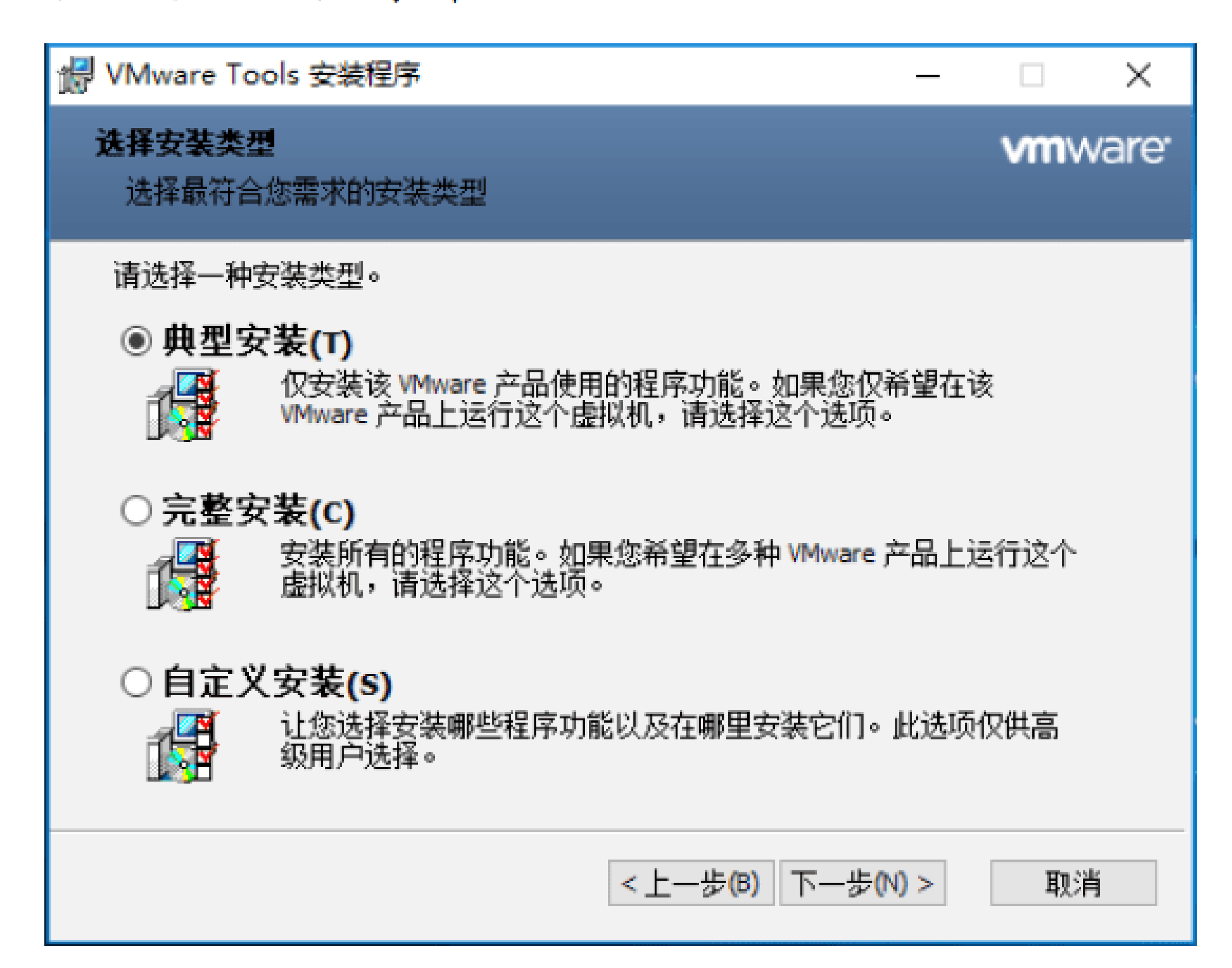
Step 02 选择“虚拟机”→“安装VMware Tools”命令，此时系统将自动弹出安装文件，如下图所示。



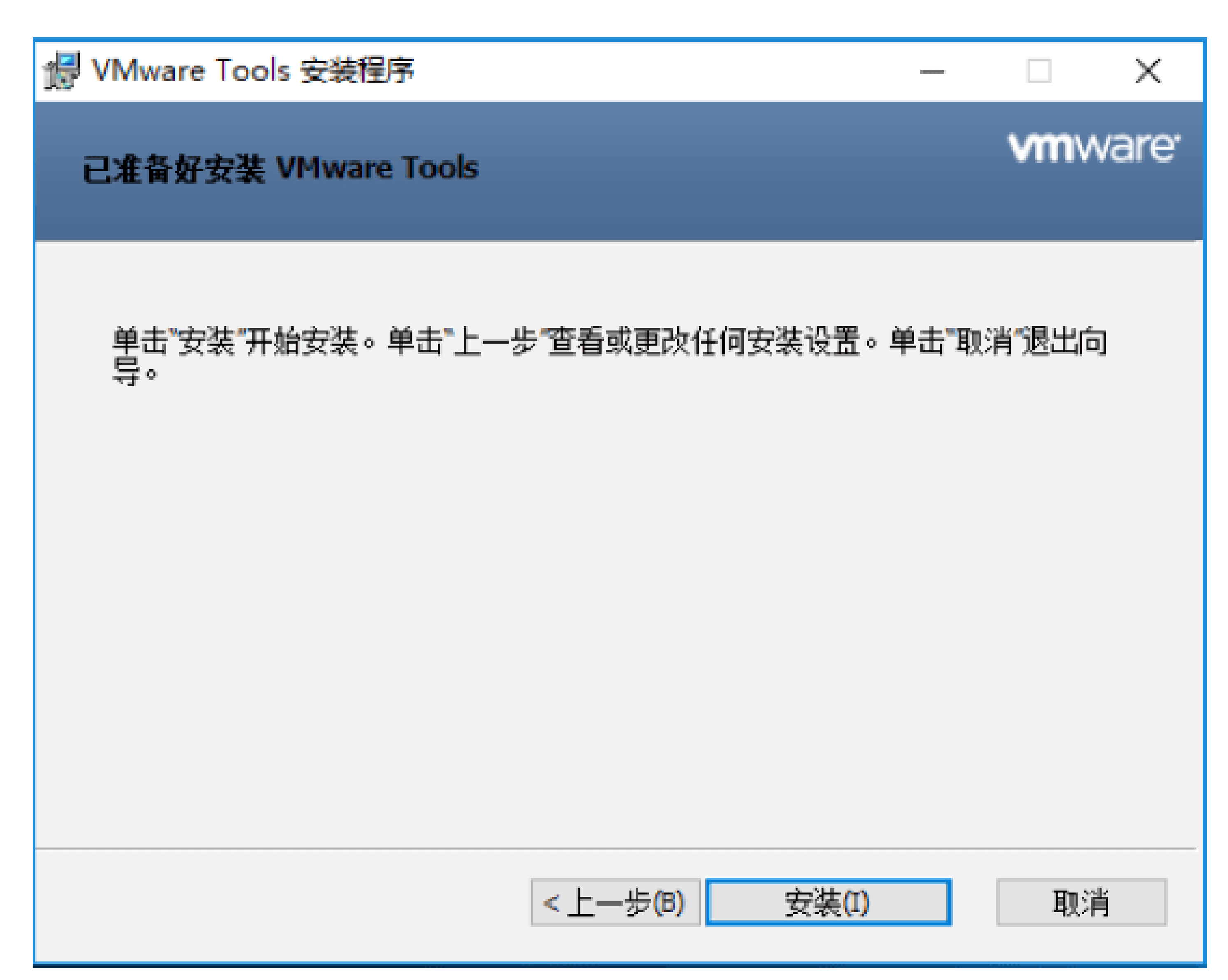
Step 03 安装文件启动之后，将会弹出“欢迎使用VMware Tools的安装向导”对话框，如下图所示。



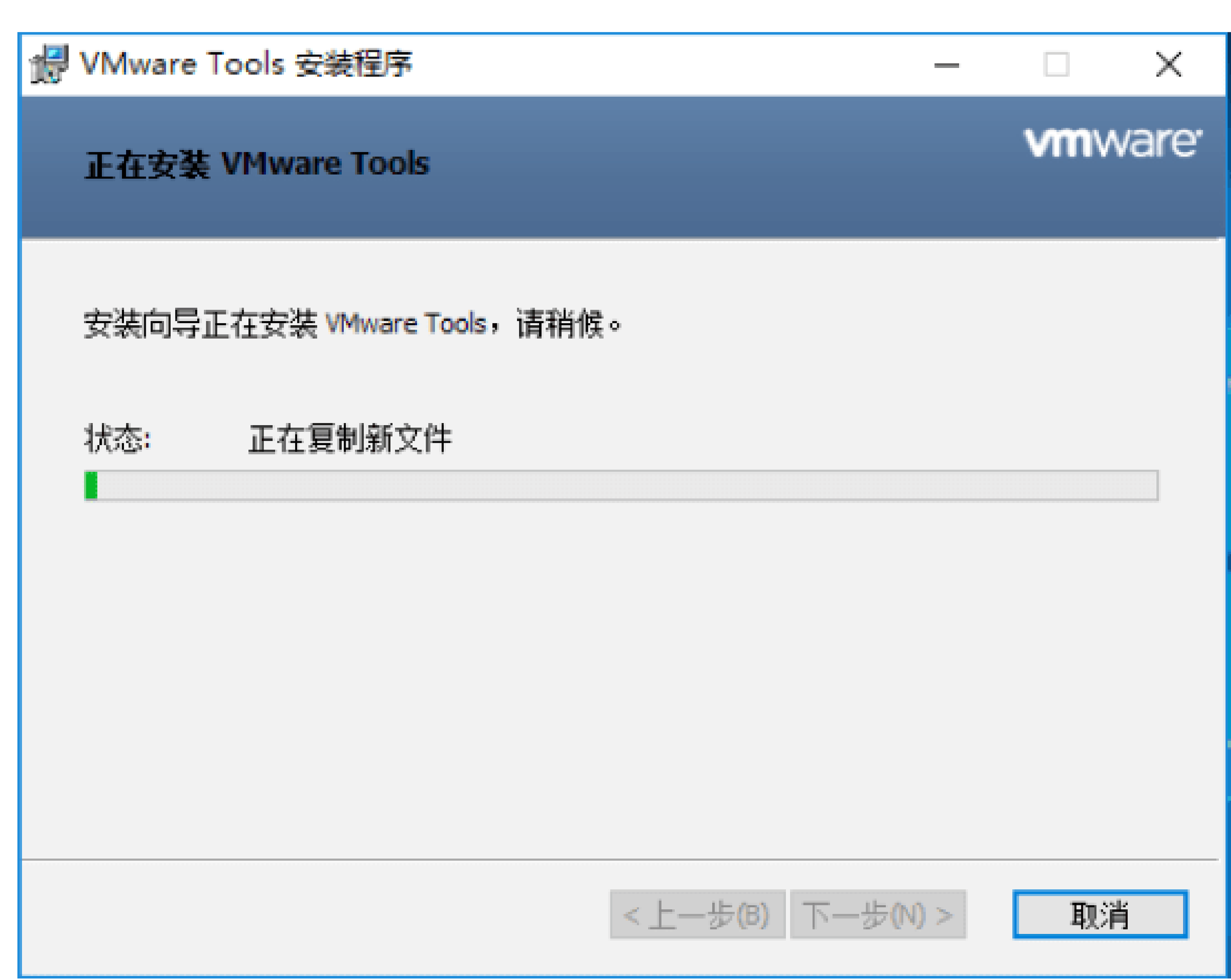
Step 04 单击“下一步”按钮，进入“选择安装类型”对话框，根据实际情况选择相应的安装类型，这里选中“典型安装”单选按钮，如下图所示。



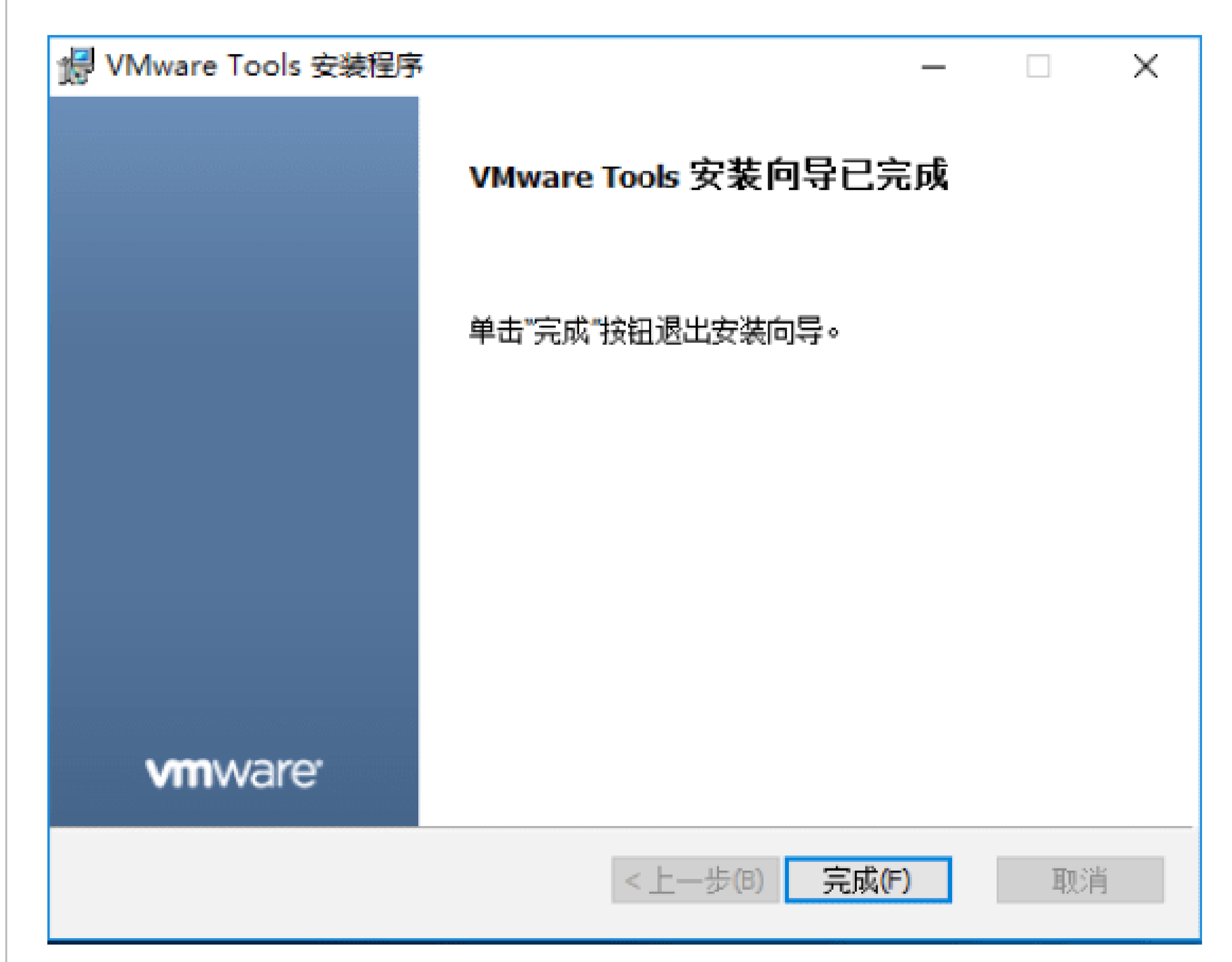
Step 05 单击“下一步”按钮，进入“已准备好安装VMware Tools”对话框，如下图所示。



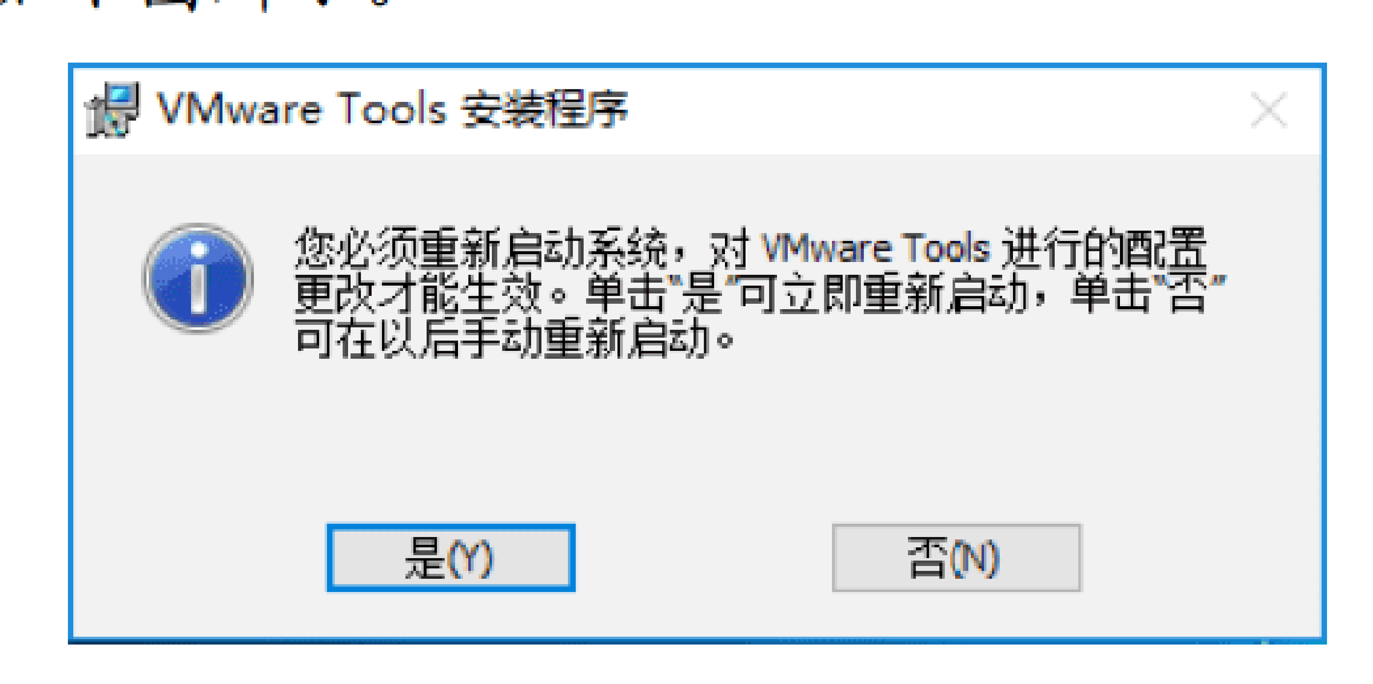
Step 06 单击“安装”按钮，进入“正在安装VMware Tools”对话框，在其中显示VMware Tools工具的安装状态，如下图所示。



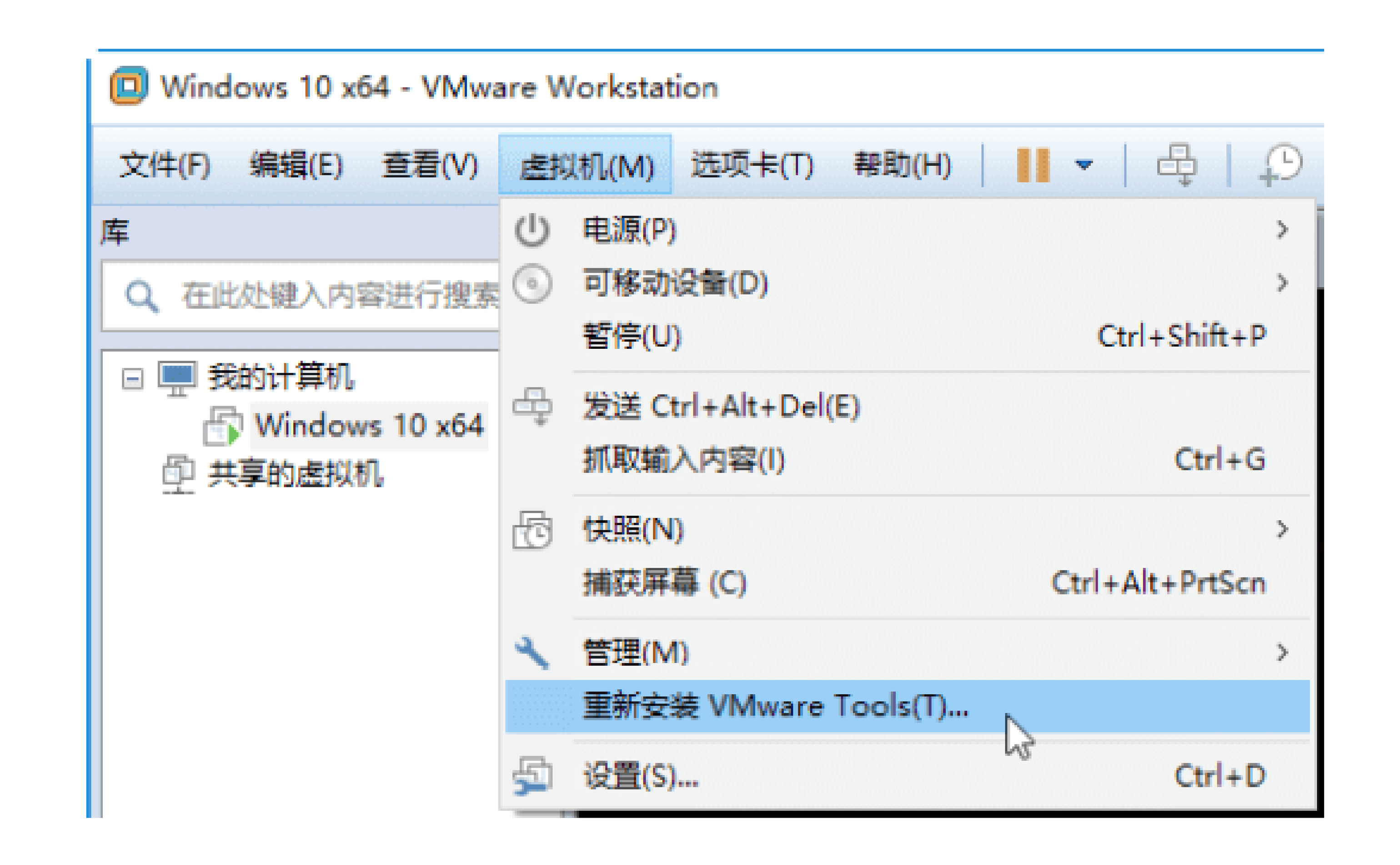
Step 07 安装完成后，进入“VMware Tools安装向导已完成”对话框，如下图所示。



Step 08 单击“完成”按钮，弹出一个信息提示框，要求必须重新启动系统，这样对VMware Tools进行的配置更改才能生效，如下图所示。



Step 09 单击“是”按钮，系统即可自动启动，虚拟系统重新启动之后即可发现虚拟机工具已经成功安装，再次选择“虚拟机”选项，可以看到“安装VMware Tools”选项变成了“重新安装VMware Tools”选项，如下图所示。



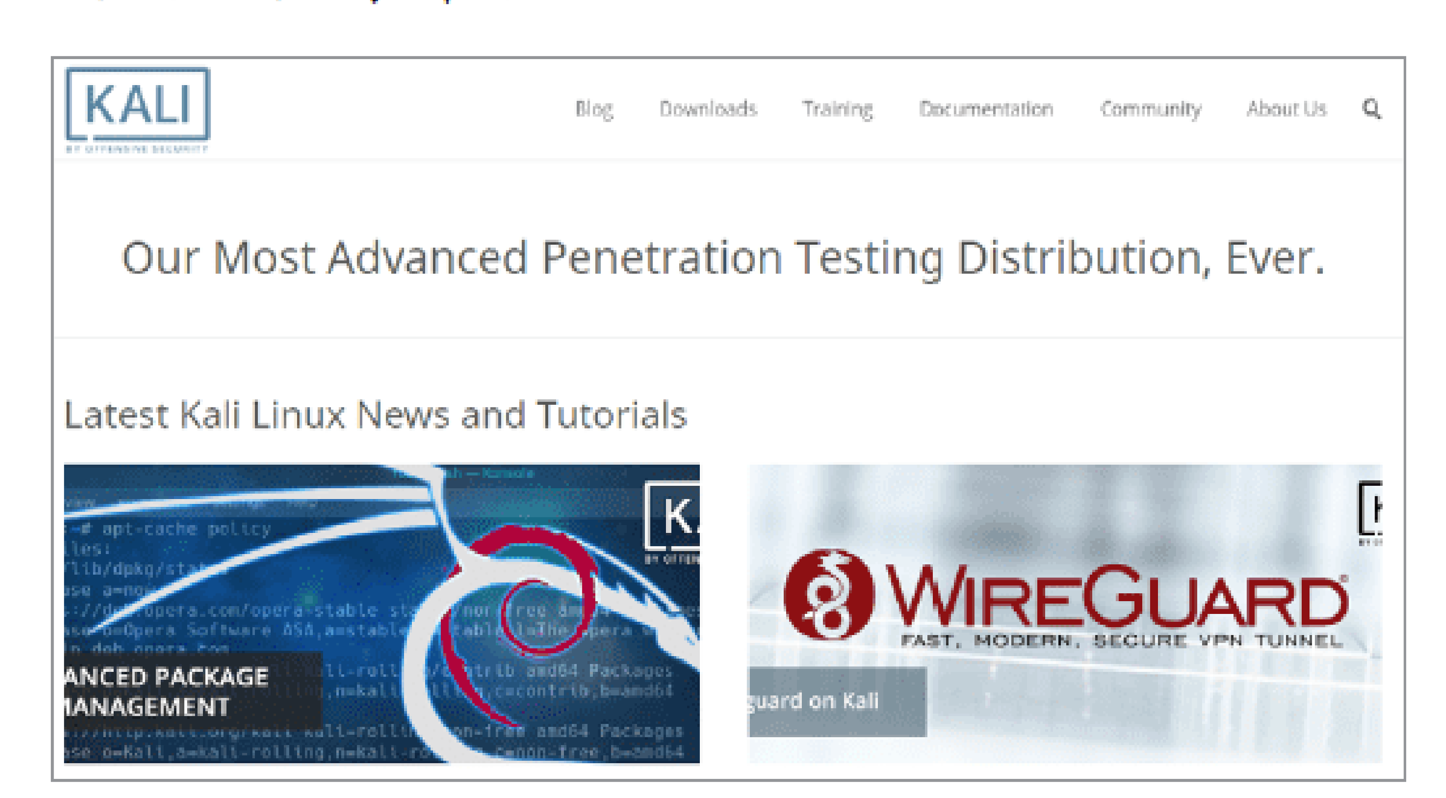
实战6：安装Kali Linux操作系统

Kali Linux是基于Debian的Linux发行版，用于数字取证操作系统，由Offensive Security Ltd维护和资助。最先由Offensive Security的Mati Aharoni和Devon Kearns通过重写BackTrack来完成，BackTrack是他们之前写的用于取证的Linux发行版 。

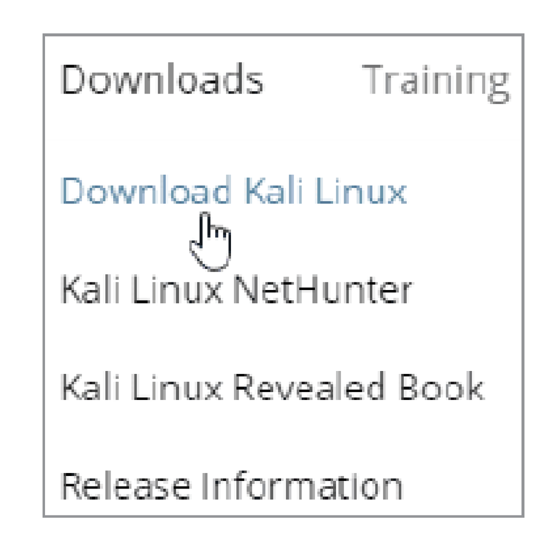
1. 下载Kali Linux系统

下载Kali Linux系统的具体操作步骤如下。

Step 01 在浏览器中输入Kali Linux系统的网址https：//www.kali.org，打开Kali官方网站，如下图所示。



Step 02 打开Downloads菜单，在弹出的菜单列表中选择Download Kail Linux选项，如下图所示。



Step 03 Kali提供了各种版本的系统下载，用户可以通过HTTP或者Torrent两种方式进行下载，如下图所示。这里选择最上面一项进行下载，用户可根据实际情况选择下载相应的版本。

Image Name	Download	Size	Version
Kali Linux 64 Bit	HTTP | Torrent	3.0G	2018.3a
Kali Linux 32 Bit	HTTP | Torrent	3.1G	2018.3a
Kali Linux Light 64 Bit	HTTP | Torrent	854M	2018.3a

Step 04 Kali官方还提供了快速装机方式，VMware镜像下载，这个列表不但提供了VMware虚拟机镜像，还提供了Vbox虚拟镜像，如下图所示。

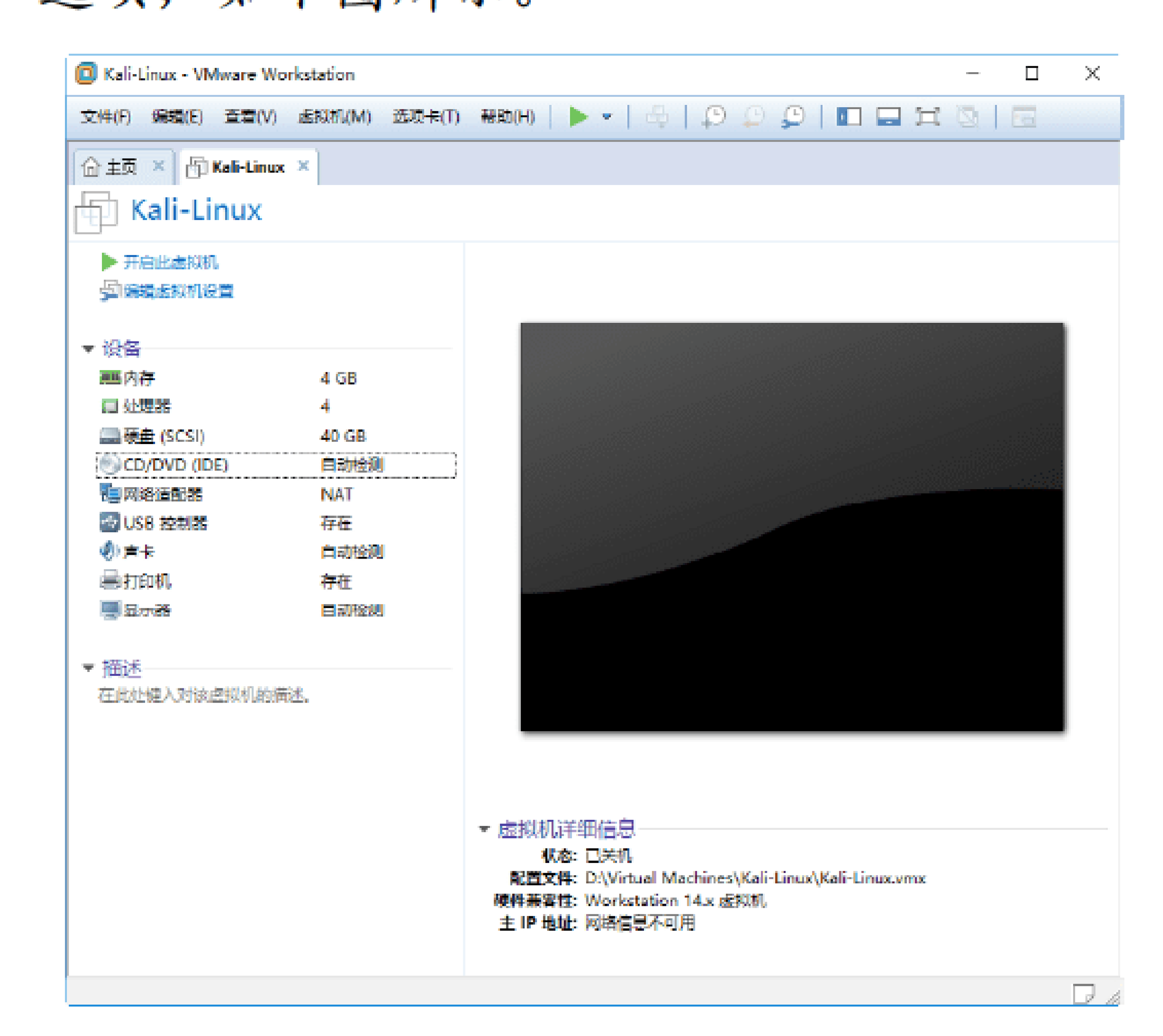


提示：初学者建议先手动安装Kali Linux系统，使用熟练后，可以选择虚拟机镜像安装。

2. 安装Kali Linux系统

架设好虚拟机并下载Kali Linux系统后，接下来便可以安装Kali Linux系统了。安装Kali Linux操作系统的具体操作步骤如下。

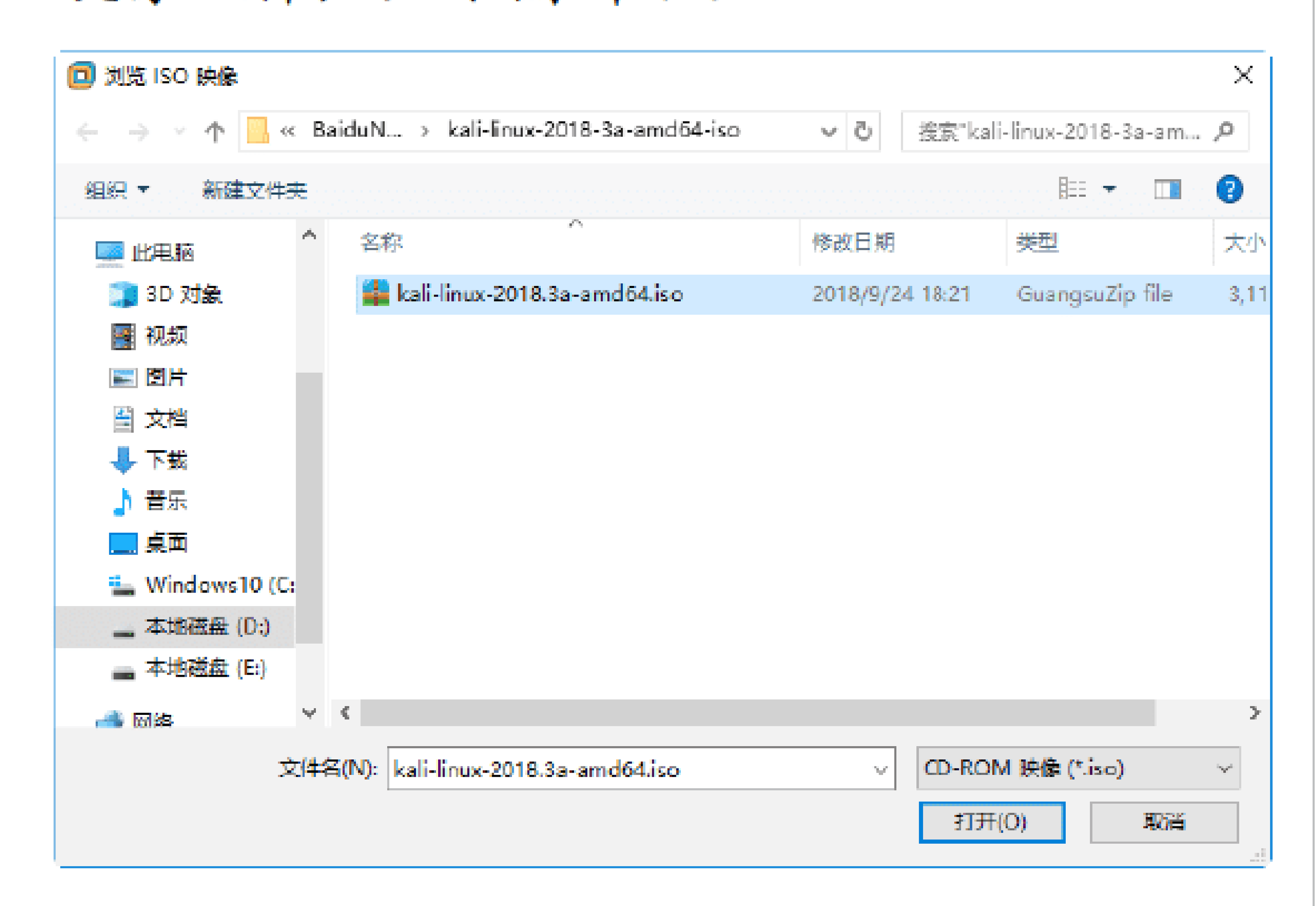
Step 01 打开安装好的虚拟机，单击CD/DVD选项，如下图所示。



Step 02 在打开的“连接”页面中选中“使用ISO映像文件”单选按钮，如下图所示。



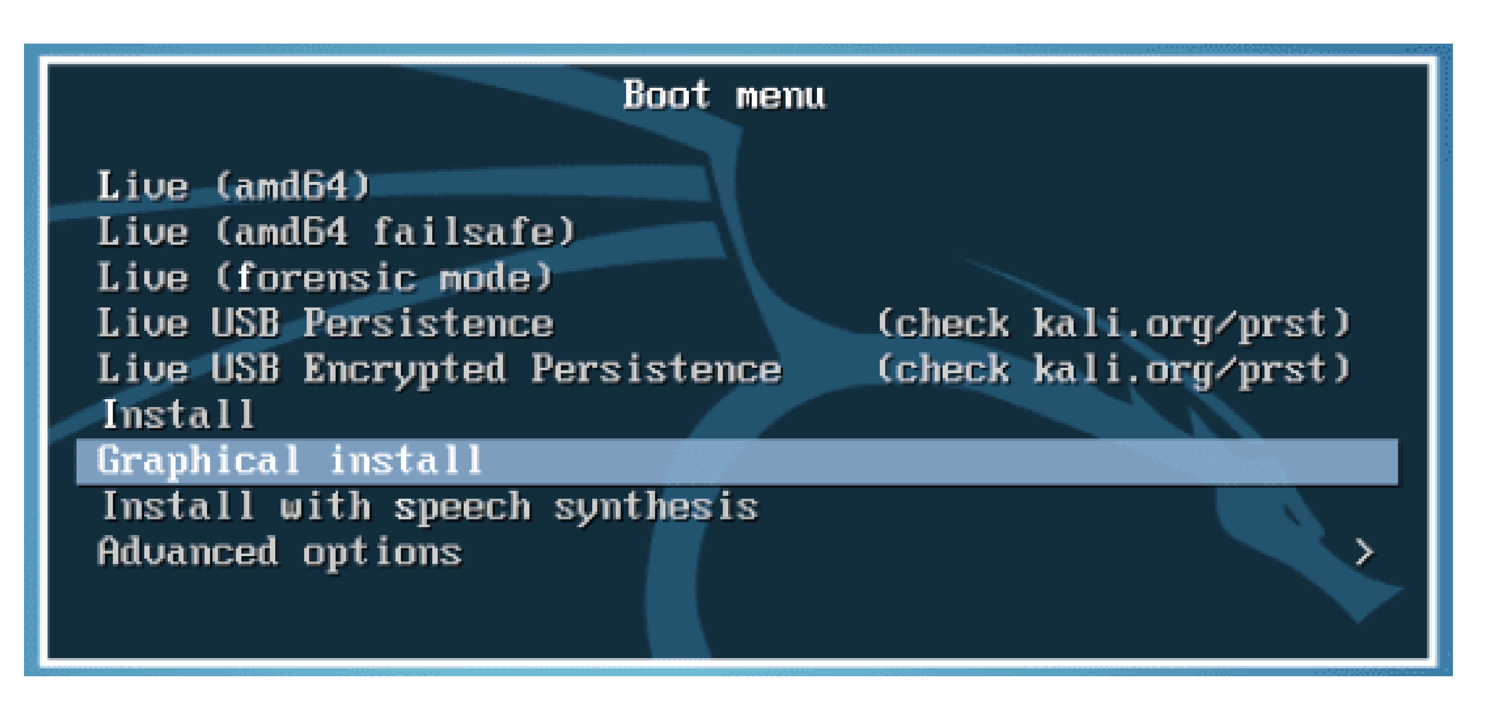
Step 03 单击“浏览”按钮，打开“浏览ISO映像”对话框，在其中选择已下载的系统映像文件，如下图所示。



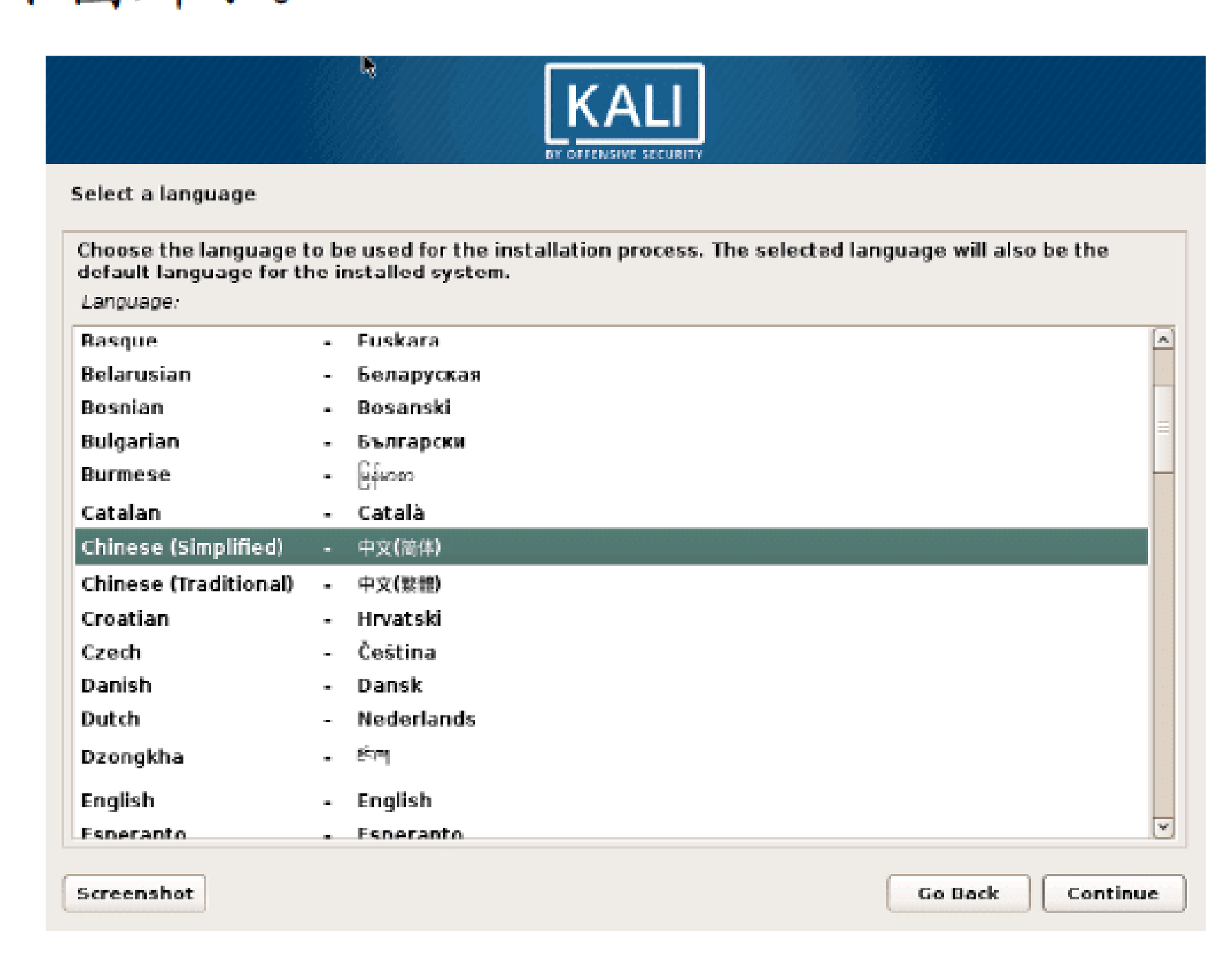
Step 04 单击“打开”按钮，返回到虚拟机设置页面，这里单击“开启此虚拟机”选项，便可以启动虚拟机，如下图所示。



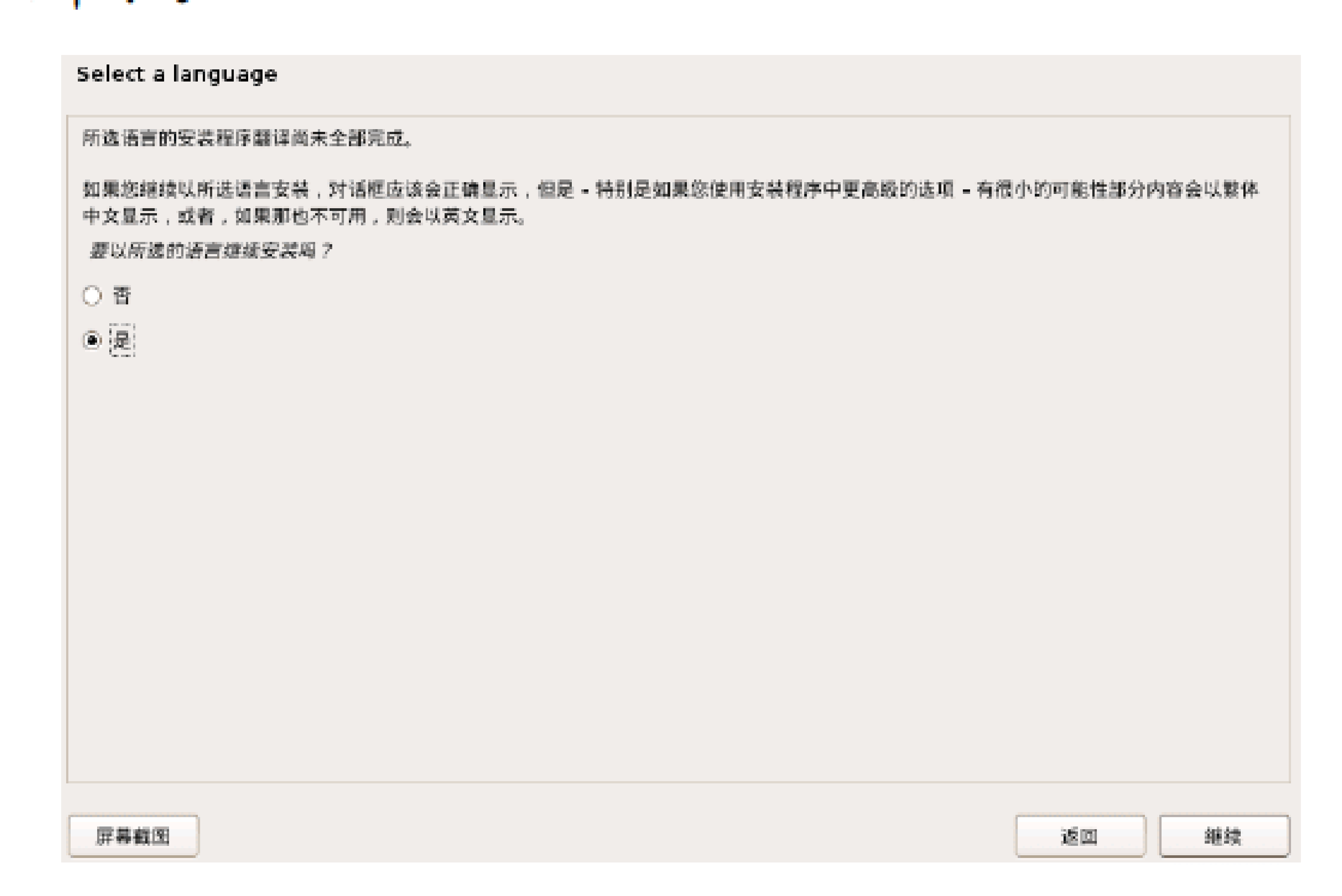
Step 05 启动虚拟机后会进入到启动选项页面，用户可以通过键盘上下键选择Graphical install选项，如下图所示。



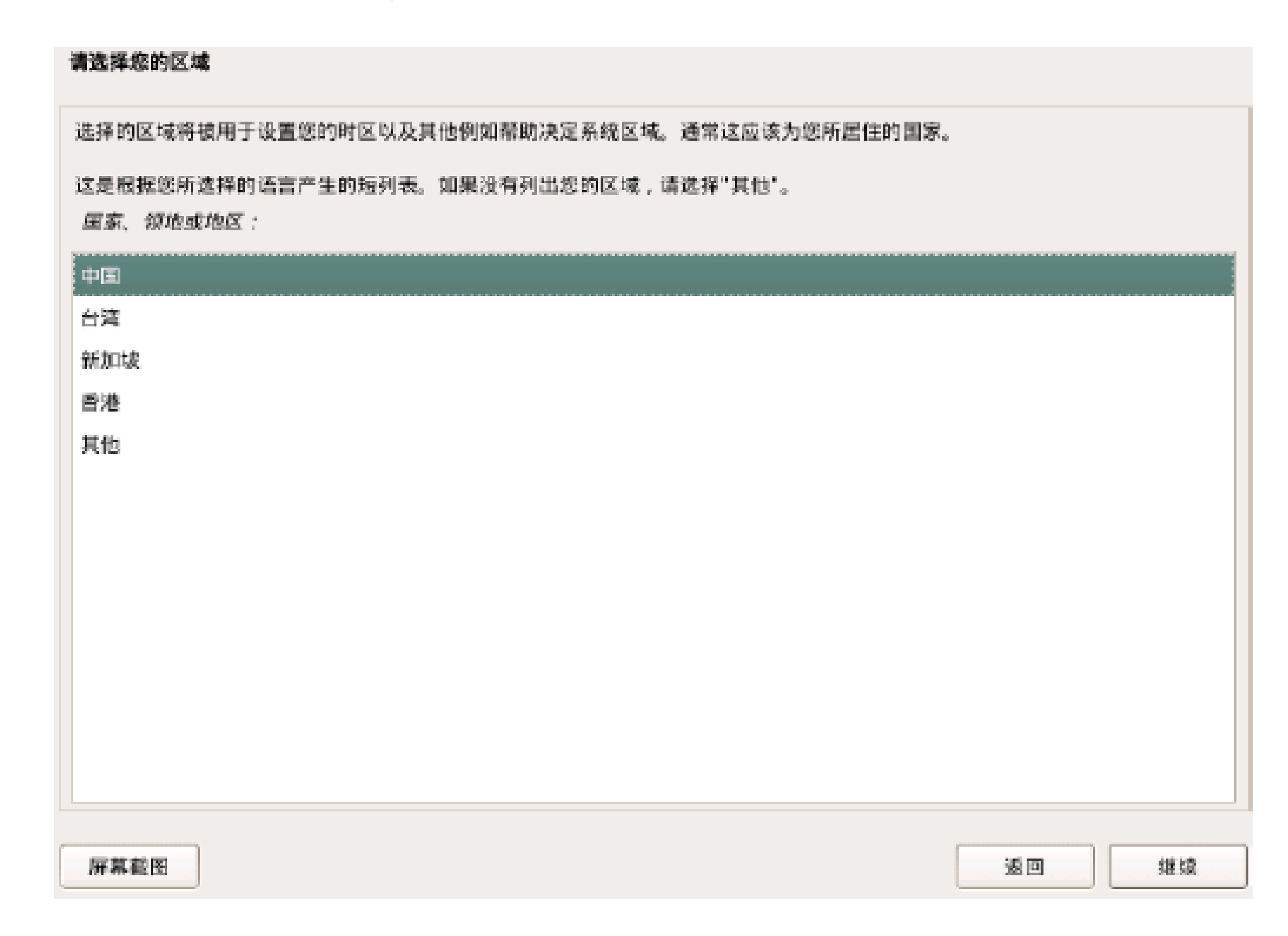
Step 06 选择完毕后，按Enter键，进入选择语言页面，这里选择“简体中文”选项，如下图所示。



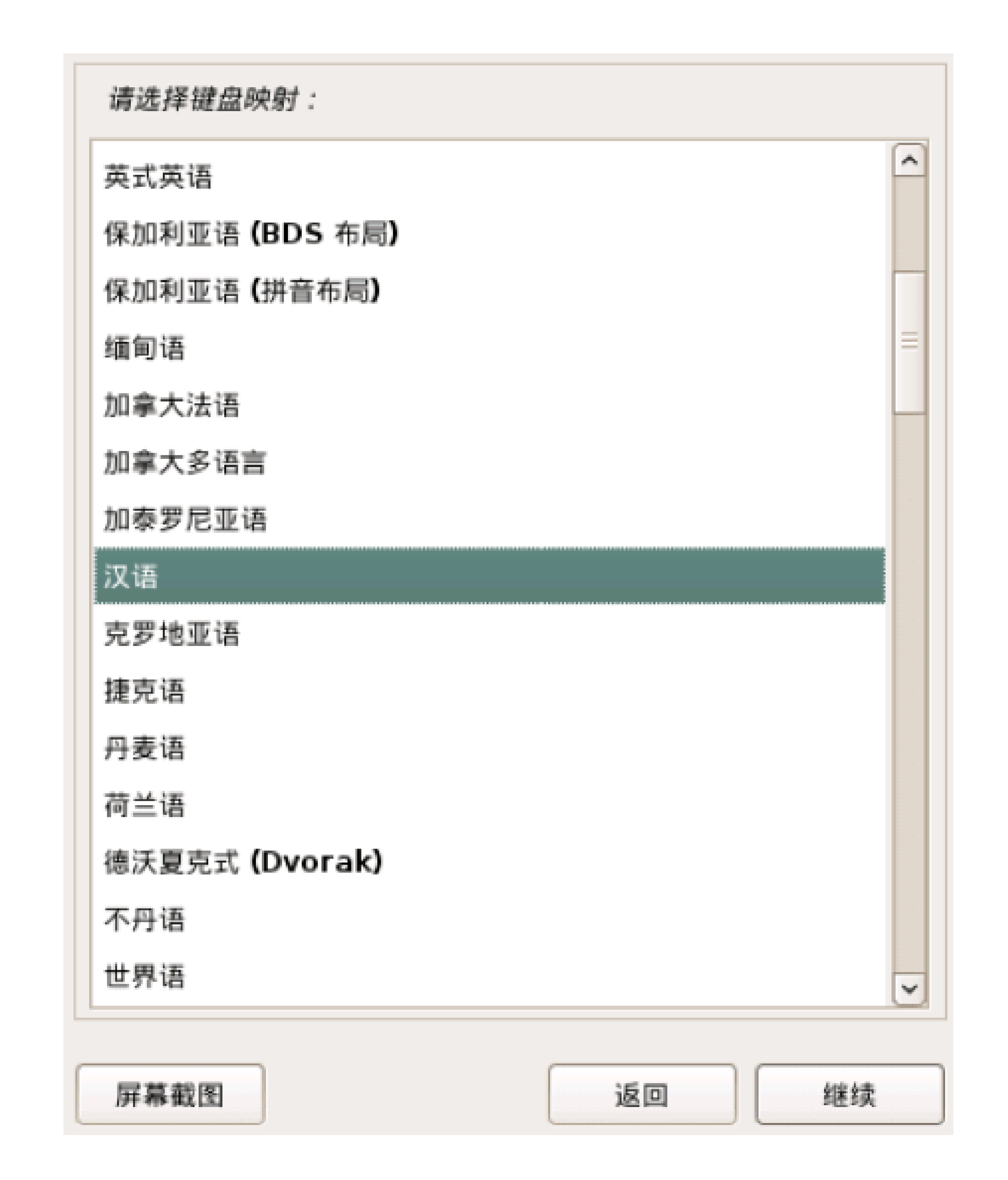
Step 07 单击Continue按钮，进入“选择语言确认”页面，保持系统默认设置，如下图所示。



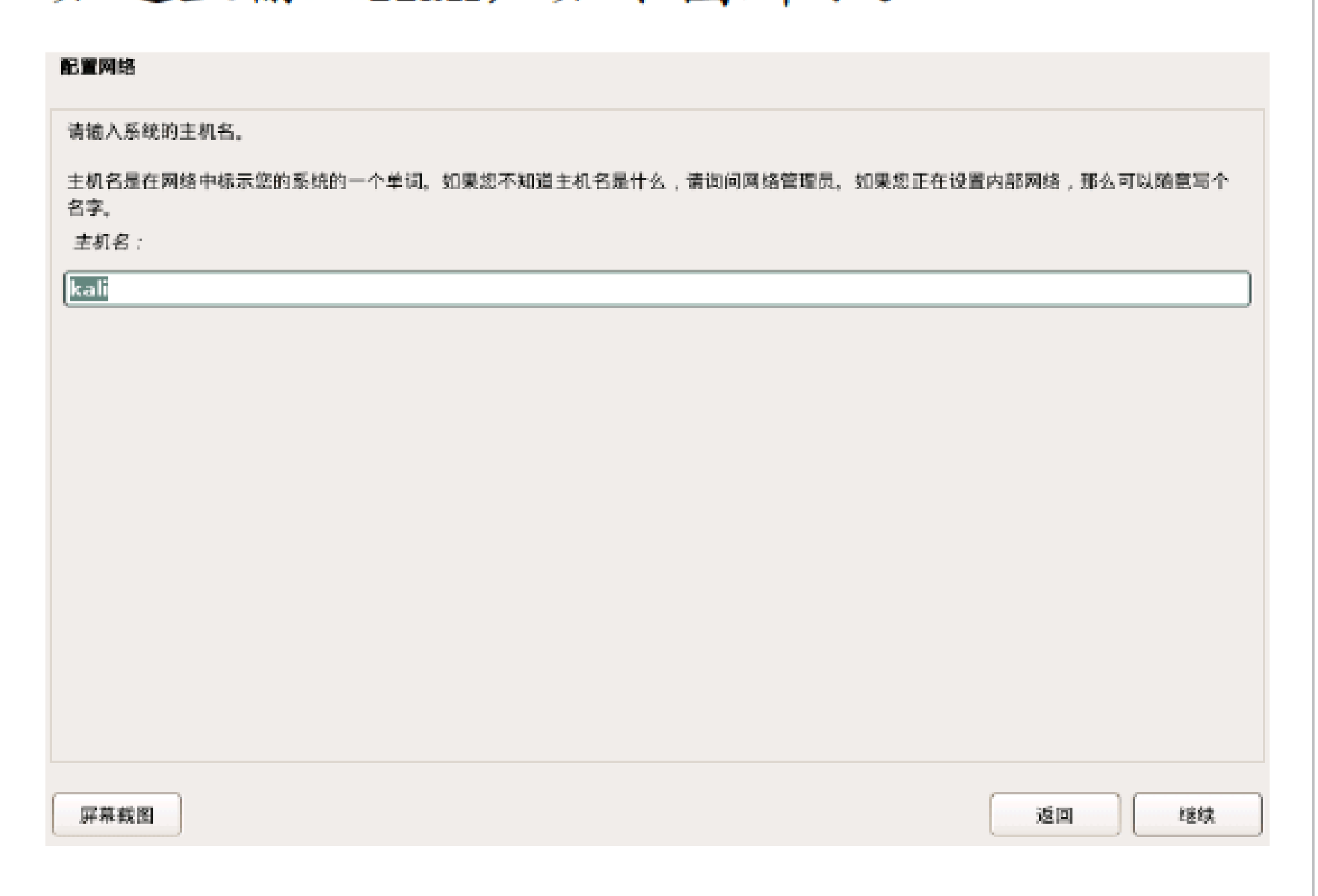
Step 08 单击“继续”按钮，进入“请选择您的区域”页面，它会自动上网匹配，即使不正确也没有关系，系统安装完成后还可以调整，这里保持默认设置，如下图所示。



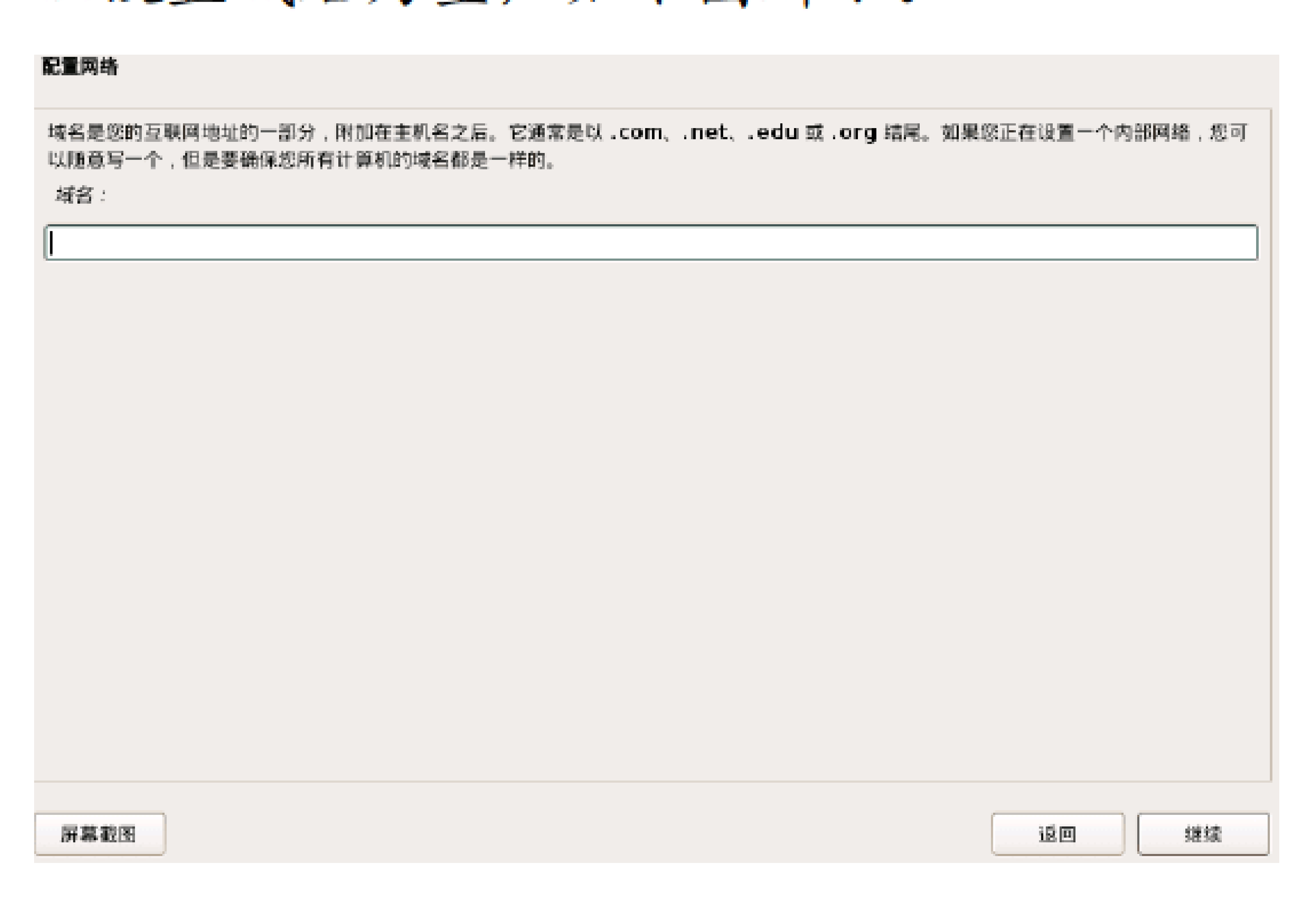
Step 09 单击“继续”按钮，进入“请选择键盘映像”页面，同样系统会根据语言选择来自行匹配，这里保持默认设置，如下图所示。



Step 10 单击“继续”按钮，进入“配置网络”页面，这里需要输入一个主机名称，如这里输入Kali，如下图所示。



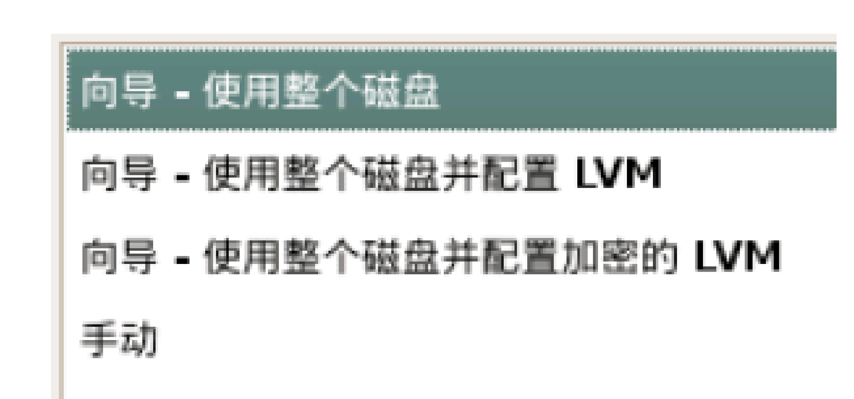
Step 11 单击“继续”按钮，进入“配置网络”页面，这里可以输入一个域名，也可以设置域名为空，如下图所示。



Step 12 按Enter键，进入设置Root管理员密码页面，这里可以设置两个相同的密码，如下图所示。



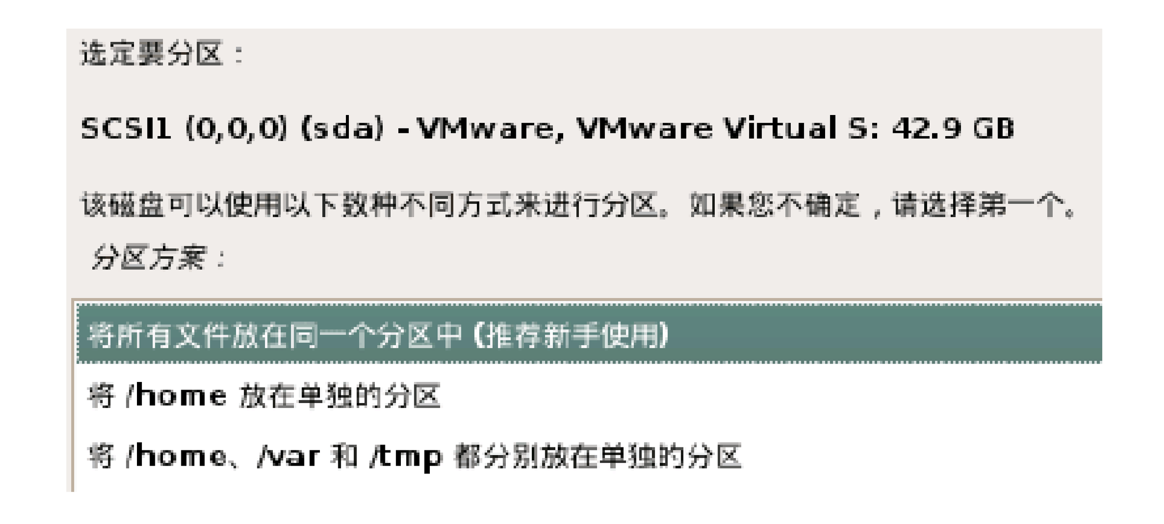
Step 13 按Enter键，进入磁盘划分页面，新手建议不划分，也就是选择“向导-使用整个磁盘”选项，如下图所示。



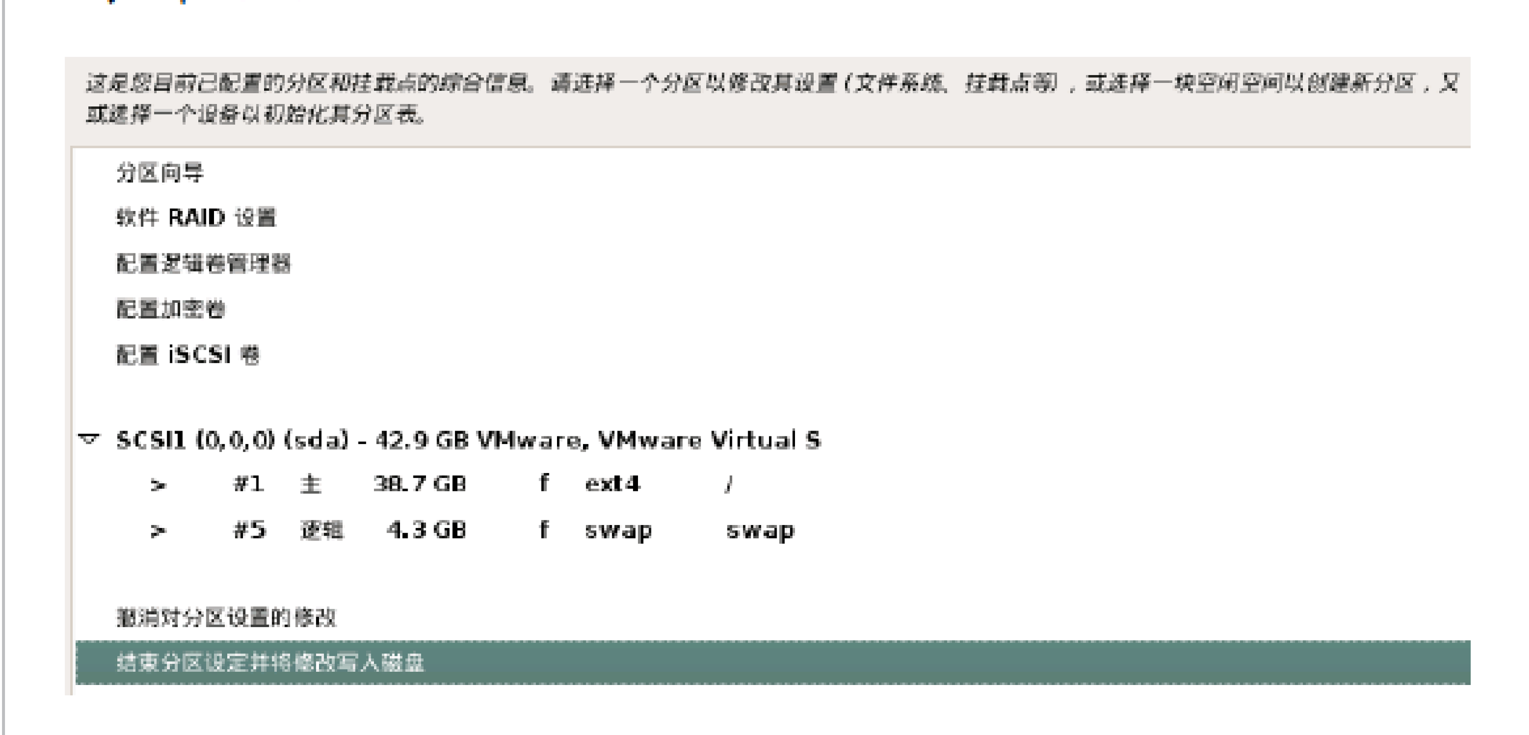
Step 14 按Enter键，进入选择分区磁盘页面，这里保持默认设置，如下图所示。



Step 15 按Enter键，进入文件分区页面，这里保持默认设置，如下图所示。



Step 16 按Enter键，进入分区确认页面，如下图所示。



Step 17 按Enter键，进入格式化分区页面，选中“是”单选按钮，如下图所示。

如果您继续，以下所列出的修改内容将会写入到磁盘中。或者，您也可以手动来进行其它修改。

以下设备的分区表已改变：
SCSI1 (0,0,0) (sda)

以下分区将被格式化：
SCSI1 (0,0,0) (sda) 设备上的第 1 分区将设为 ext4
SCSI1 (0,0,0) (sda) 设备上的第 5 分区将设为 swap

将改动写入磁盘吗？

○ 否

◉ 是

Step 18 按Enter键，进入配置软件包管理器页面，这里保持默认设置，如下图所示。

网络镜像可以用来补充光盘所带的软件，也可以用来提供较新版本的软件。

使用网络镜像吗？

○ 否

◉ 是

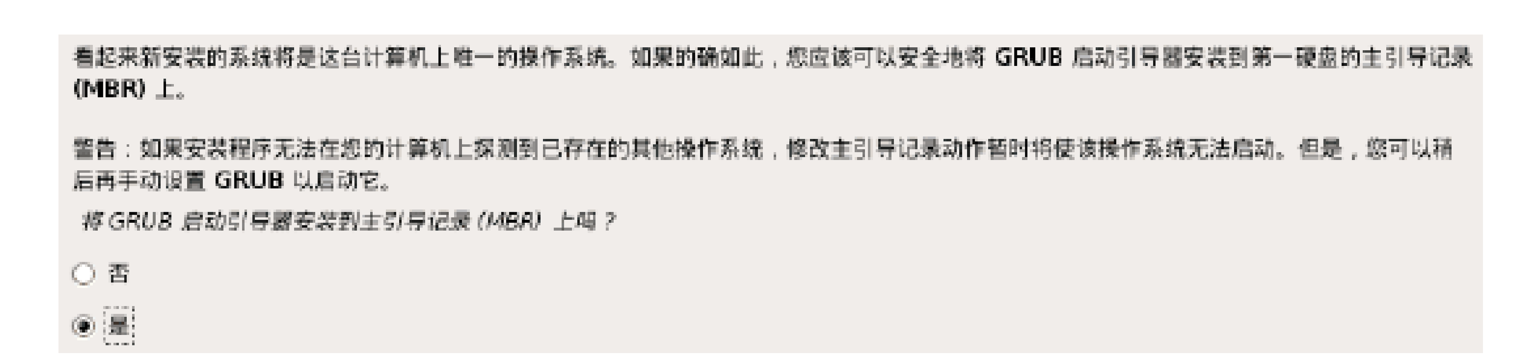
Step 19 按Enter键，进入是否使用代理上网页面，保持默认设置，如下图所示。

如果您需要用 HTTP 代理来连接外部网络，请在此输入代理信息。否则，请置空。

代理信息应按照“http://[[用户名][:密码]@]主机名[:端口]/”的标准格式给出。

HTTP 代理信息（如果没有请留空）：

Step 20 按Enter键，进入将GRUB安装至硬盘页面，保持默认设置，如下图所示。



Step 21 按Enter键，进入选择引导路径页面，选择“/dev/sda”选项，如下图所示。

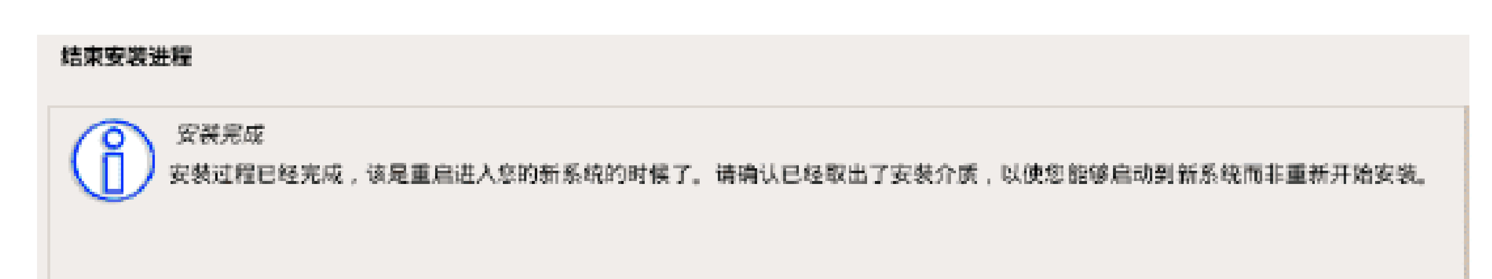
您需要通过将 GRUB 启动引导器安装到可启动设备上以使新安装的系统能够启动。通常的作法是将 GRUB 安装到您第一块硬盘的主引导记录 (MBR) 上。如果您愿意，也可以将 GRUB 安装到驱动器的其他地方，或者其他的驱动器上，甚至还可以安装到一张软盘上。

安装启动引导器的设备：

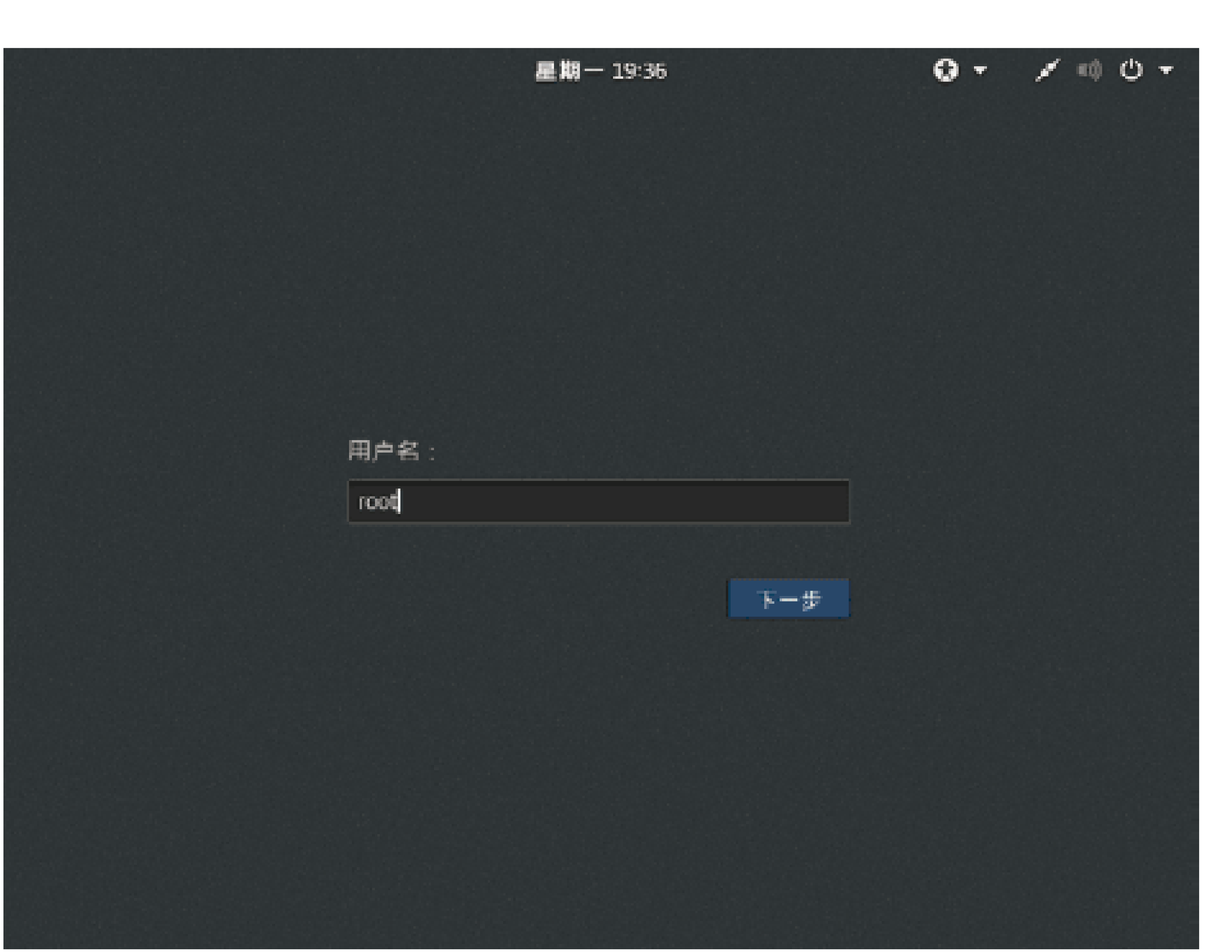
手动输入设备

/dev/sda

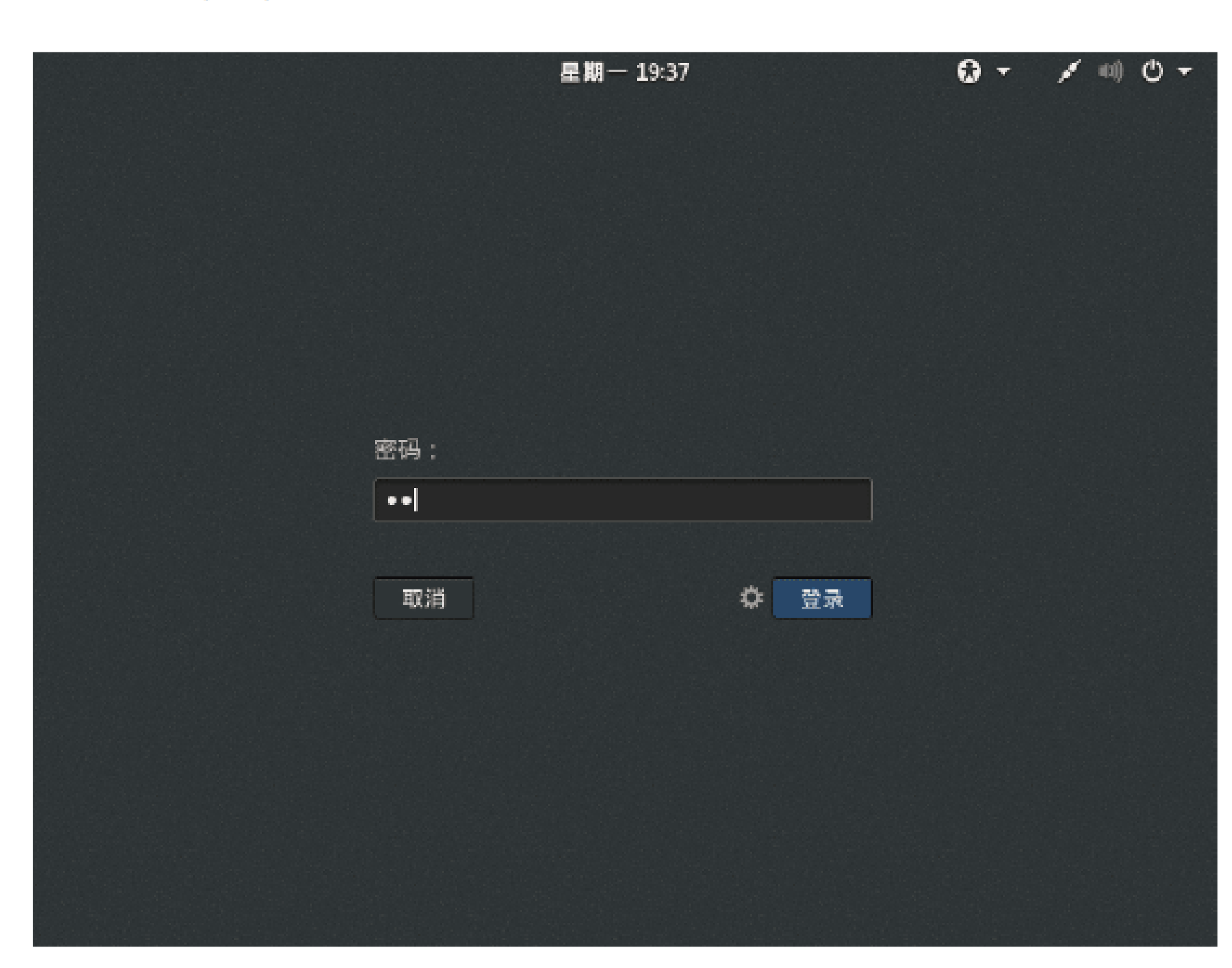
Step 22 按Enter键，完成安装，提示用户重启进入系统，如下图所示。



Step 23 按Enter键，安装完成后重启，进入“用户名”页面，在其中输入Root管理员账号，如下图所示。



Step 24 单击“下一步”按钮，进入登录密码页面，在其中输入设置好的管理员密码，如下图所示。



Step 25 单击“登录”按钮，至此便完成了整个Kail Linux系统的安装工作，如下图所示。

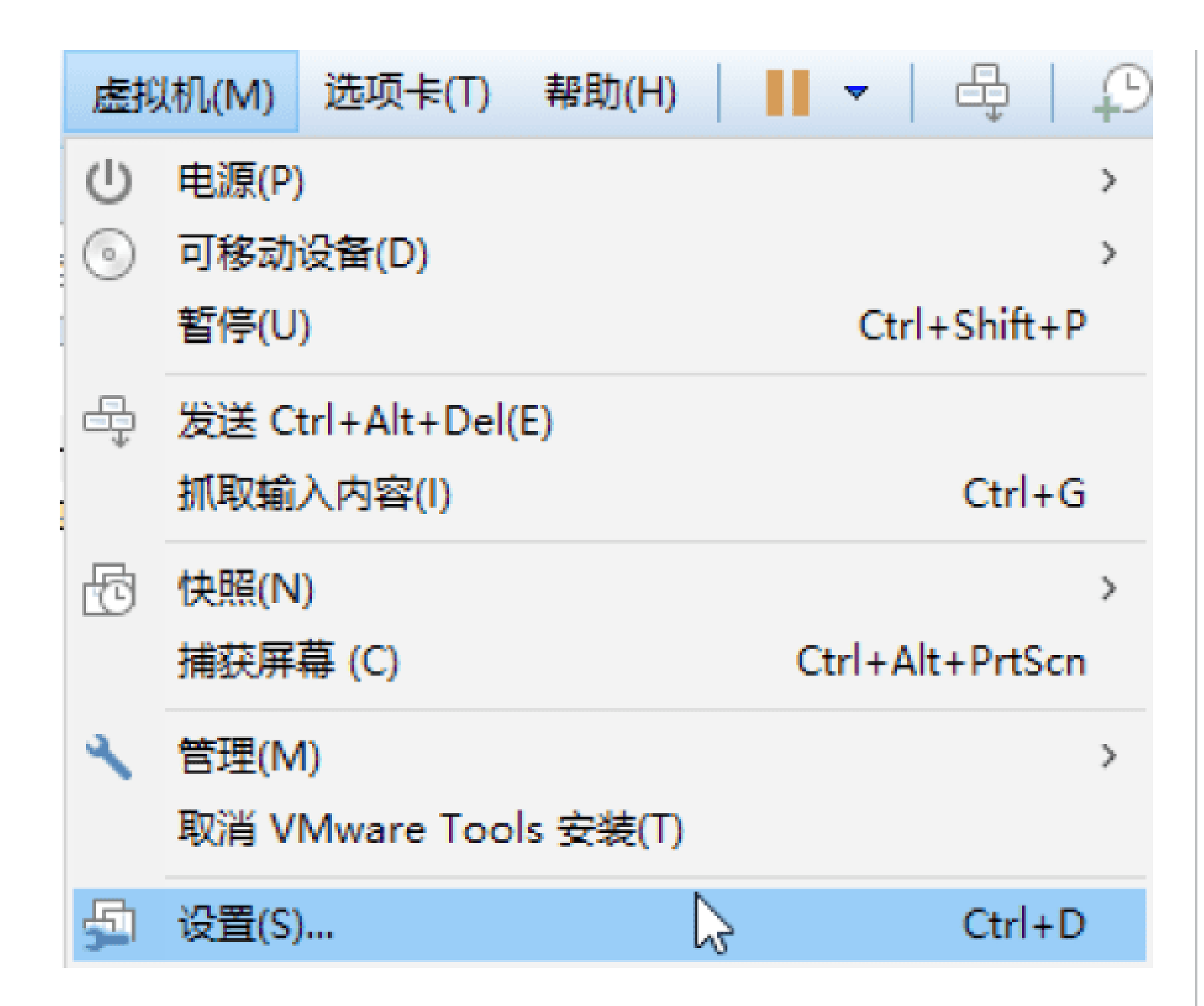


2.4　实战演练

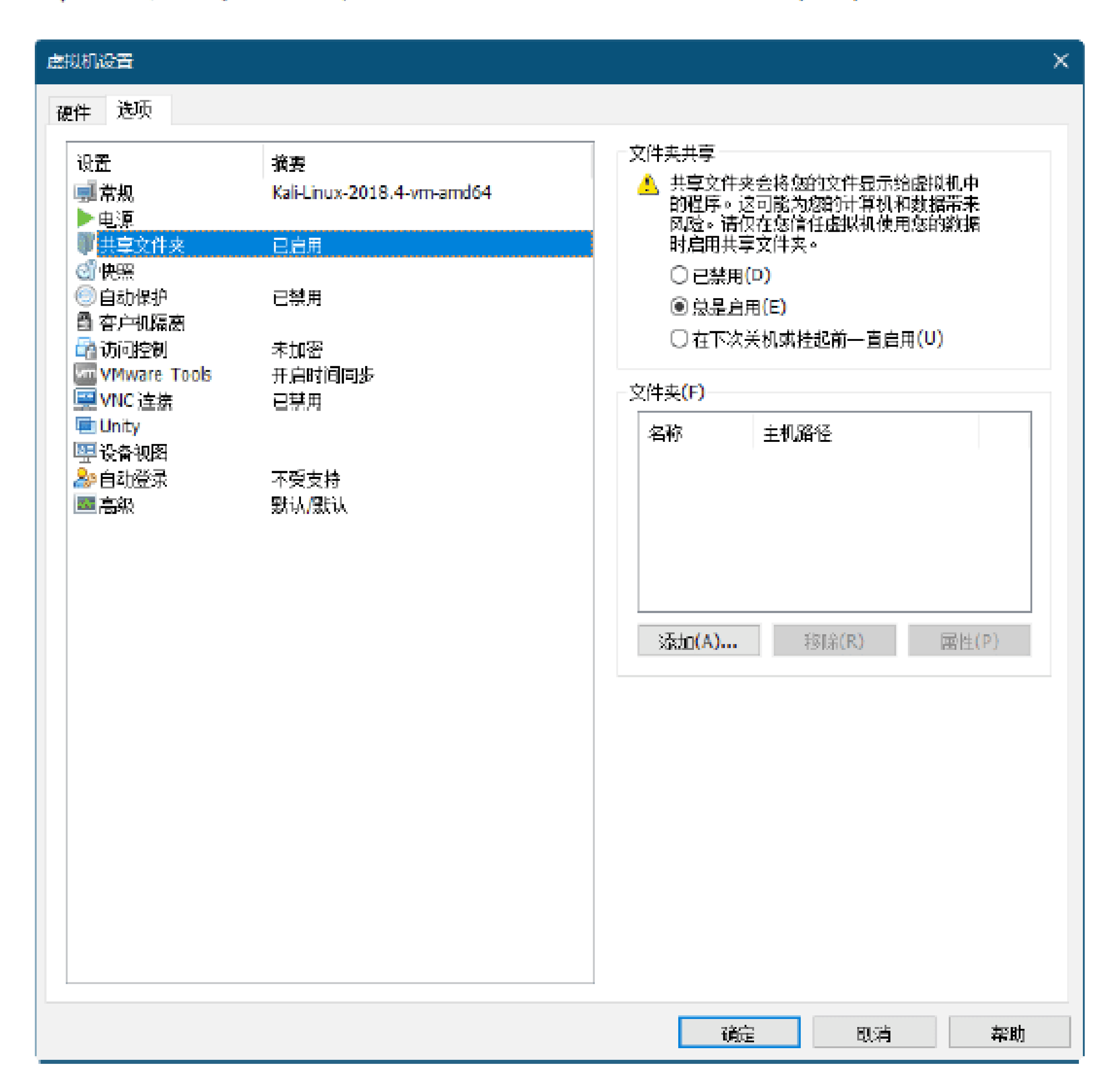
实战演练1——设置Kail与主机共享文件夹

通过安装虚拟机工具，设置Kali与主机实现共享文件夹。具体操作步骤如下。

Step 01 在VMware工具栏中，选择“虚拟机”菜单项，在弹出的菜单列表中选择“设置”选项，如下图所示。



Step 02 打开“虚拟机设置”对话框，选择“选项”选项卡，并在“设置”列表中选择“共享文件夹”选项，如下图所示。



Step 03 单击“添加”按钮，弹出“添加共享文件夹向导”对话框，如下图所示。



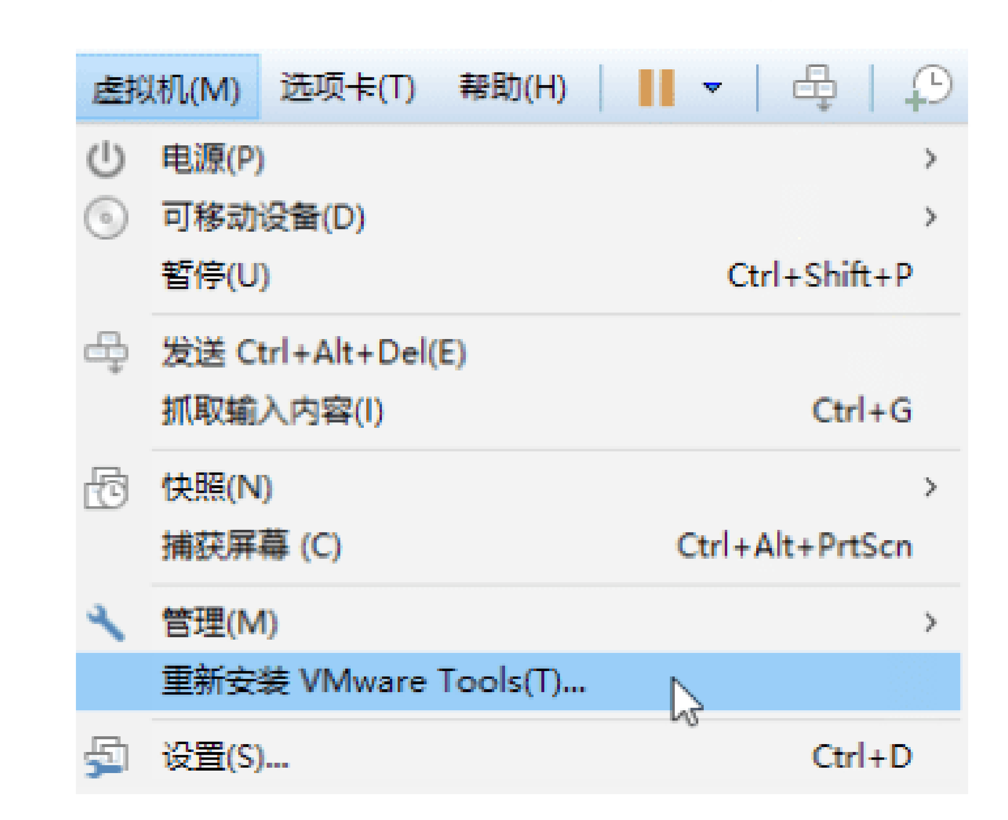
Step 04 单击“下一步”按钮，在打开的“命名共享文件夹”对话框中输入文件夹名称，并选择一个共享文件夹路径，如下图所示。



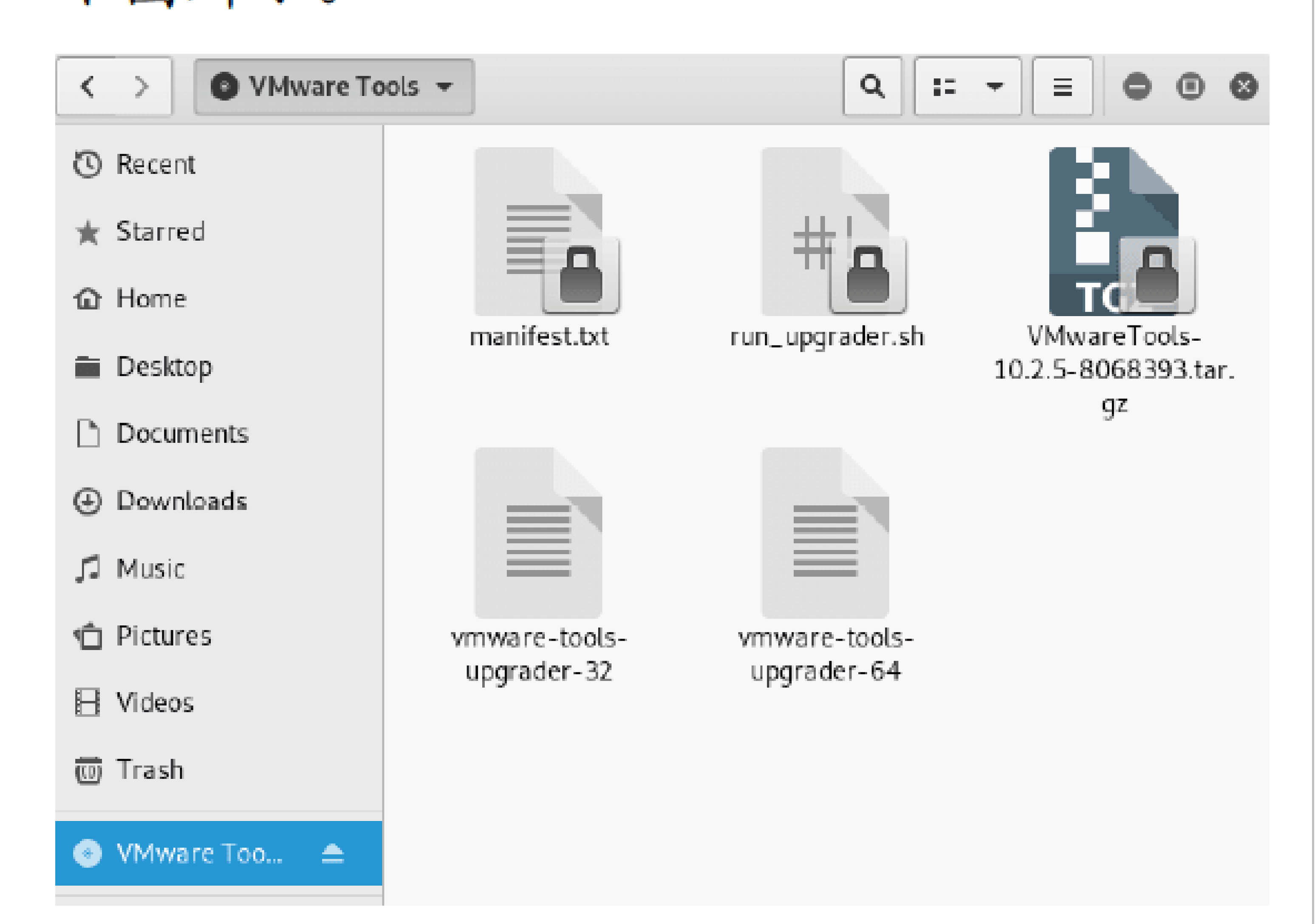
Step 05 单击“下一步”按钮，进入“指定共享文件夹属性”对话框，指定共享文件夹属性，也可以保持默认设置，最后单击“完成”按钮，完成共享文件夹的设置操作，如下图所示。



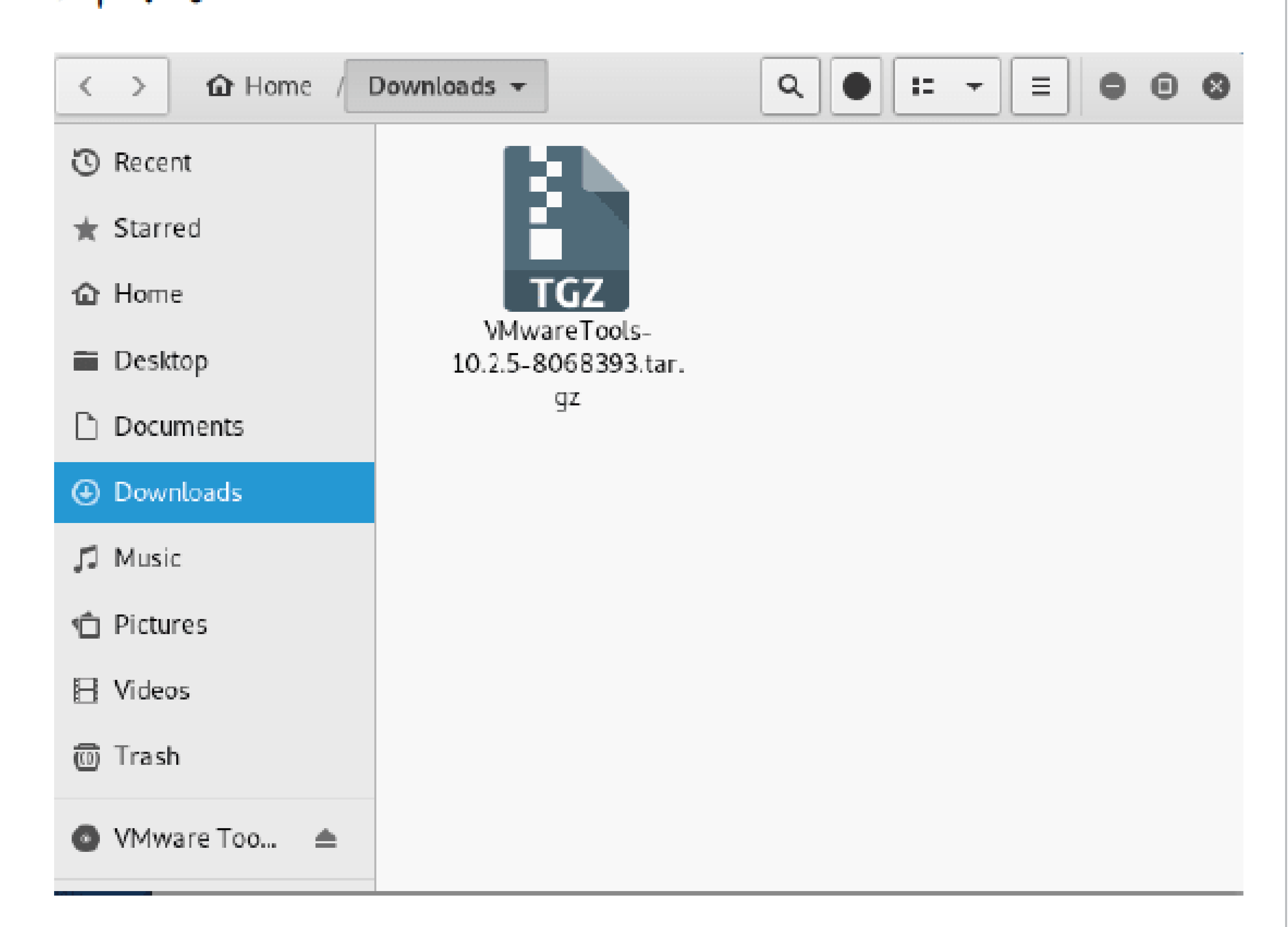
Step 06 在VMware菜单中选择“虚拟机”选项，在弹出的菜单列表中选择“重新安装VMware Tools”选项，如下图所示。



Step 07 此时会在Kali虚拟机中弹出一个安装光盘，打开光盘后，里面会有5个文件，如下图所示。



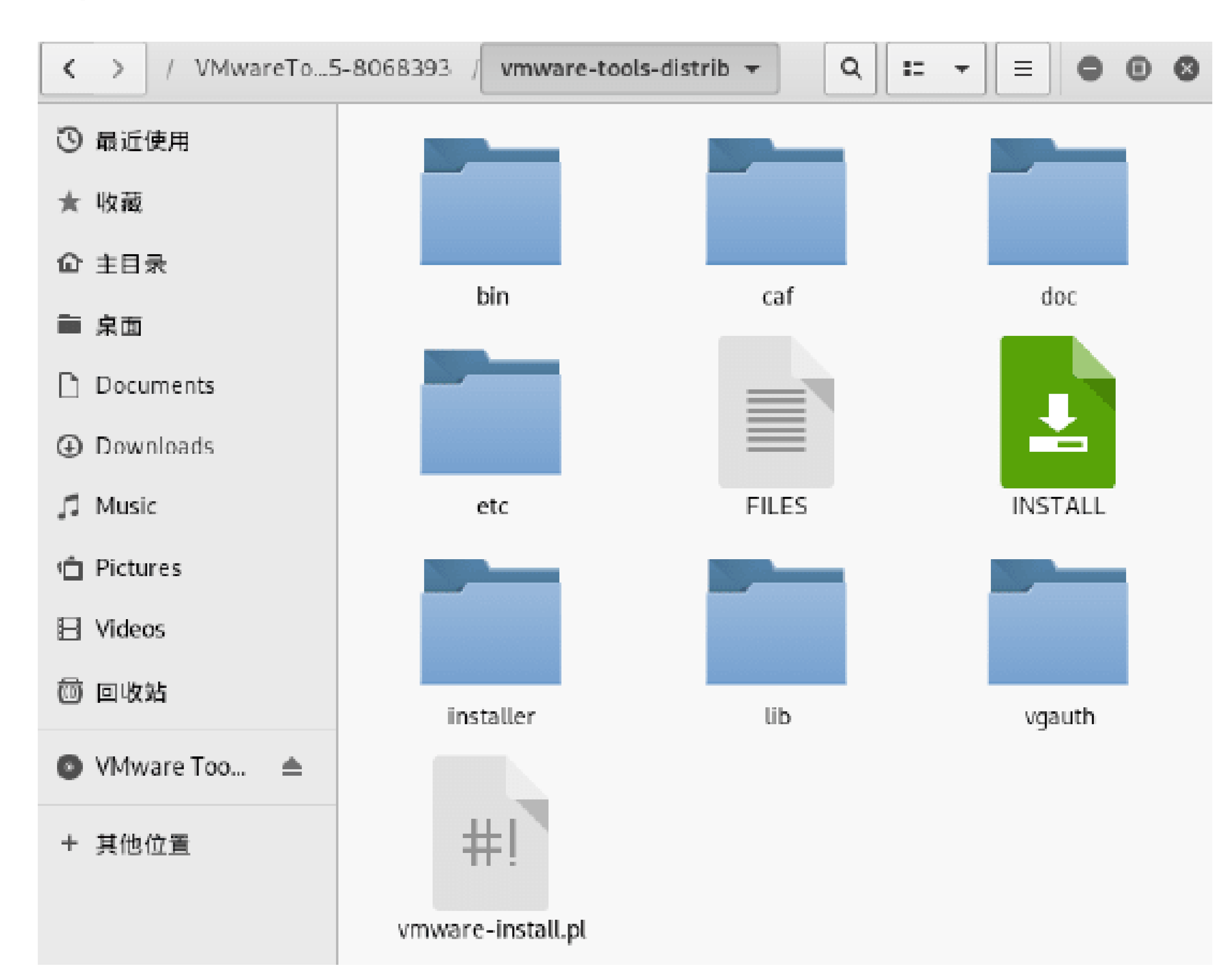
Step 08 复制压缩包文件VMwareTools -10.2.5 -8068393.tar.gz到Downloads目录下，如下图所示。



Step 09 选中压缩包文件，单击鼠标右键，在弹出的快捷菜单中选择“提取到此处”选项，如下图所示。



Step 10 开始解压文件夹，解压完成后，在内部发现一个vmware-install.pl文件，如下图所示。



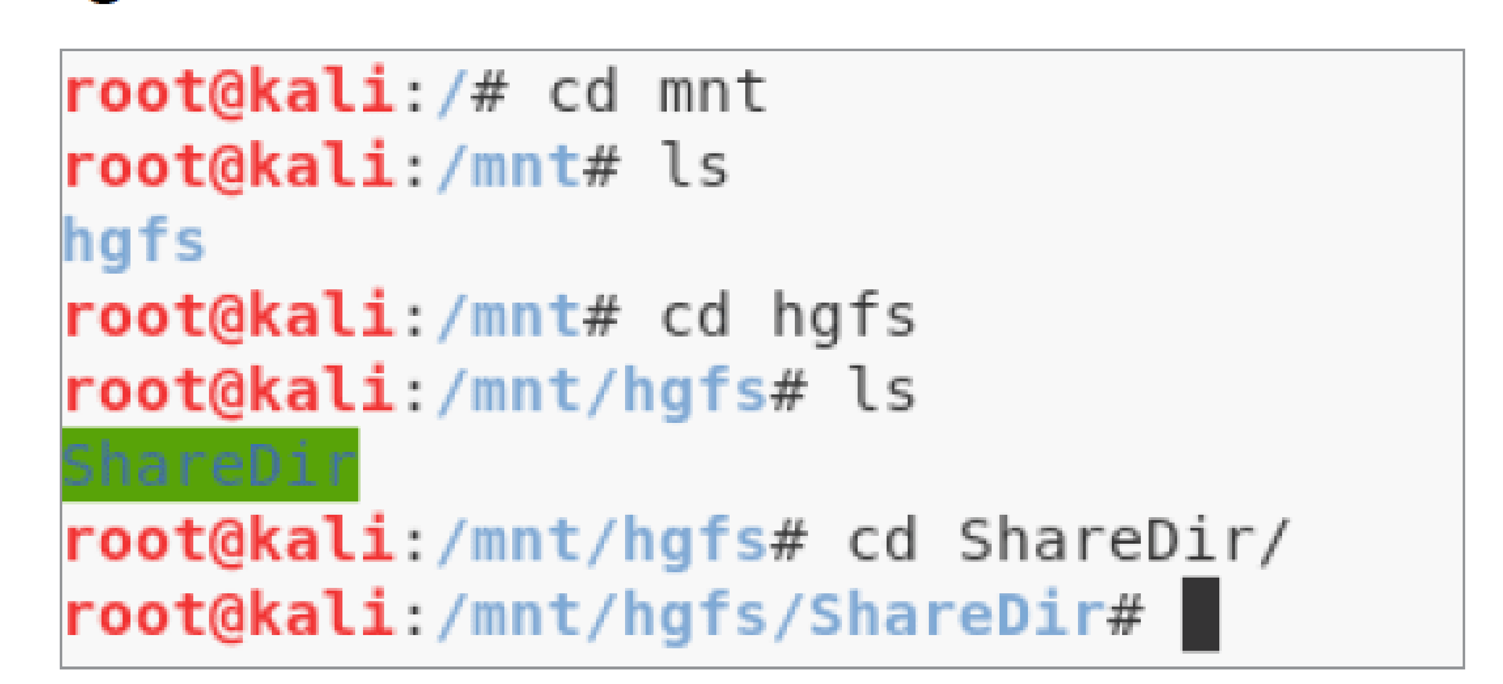
Step 11 鼠标移动到文件夹空白区域，单击鼠标右键，在弹出的快捷菜单中选择“在终端打开”选项，如下图所示。



Step 12 这时，在终端中执行./ vmware-install.pl命令，结果如下图所示。

```
root@kali:~/Downloads/VMwareTools-10.2.5-8068393/vmware-tools-distrib# ./vmware-install.pl
The installer has detected an existing installation of open-vm-tools packages
on this system and will not attempt to remove and replace these user-space
applications. It is recommended to use the open-vm-tools packages provided by
the operating system. If you do not want to use the existing installation of
open-vm-tools packages and use VMware Tools, you must uninstall the
open-vm-tools packages and re-run this installer.
The packages that need to be removed are:
open-vm-tools
Packages must be removed with the --purge option.
The installer will next check if there are any missing kernel drivers. Type yes
if you want to do this, otherwise type no [yes] y
```

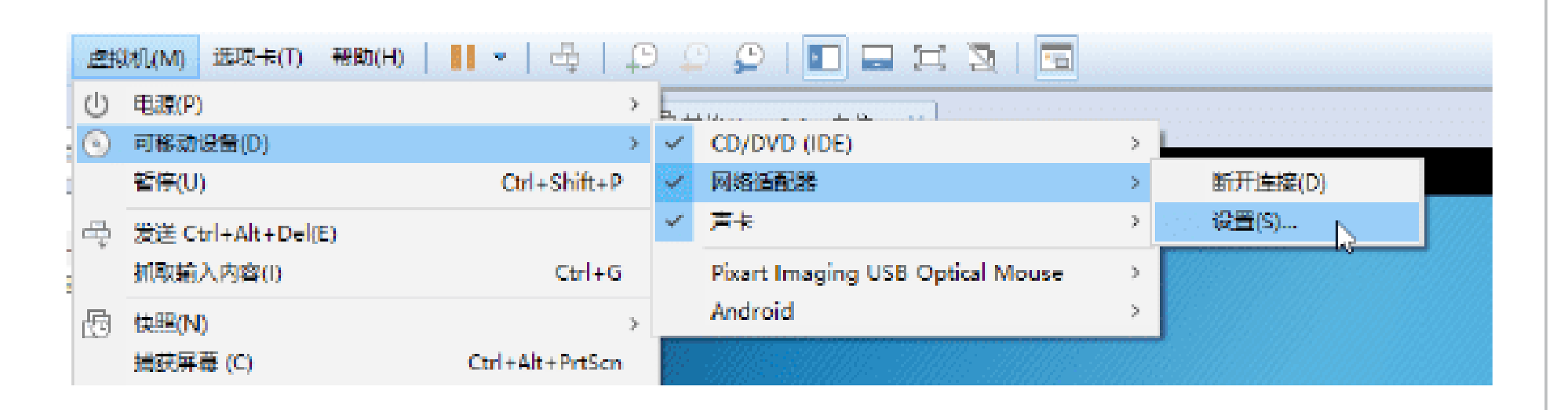
Step 13 如果安装过程中提示[yes]，按键盘上的y键或Enter键，直到安装完成，安装完成后，在mnt目录中会多出一个共享文件夹hgfs，如下图所示。



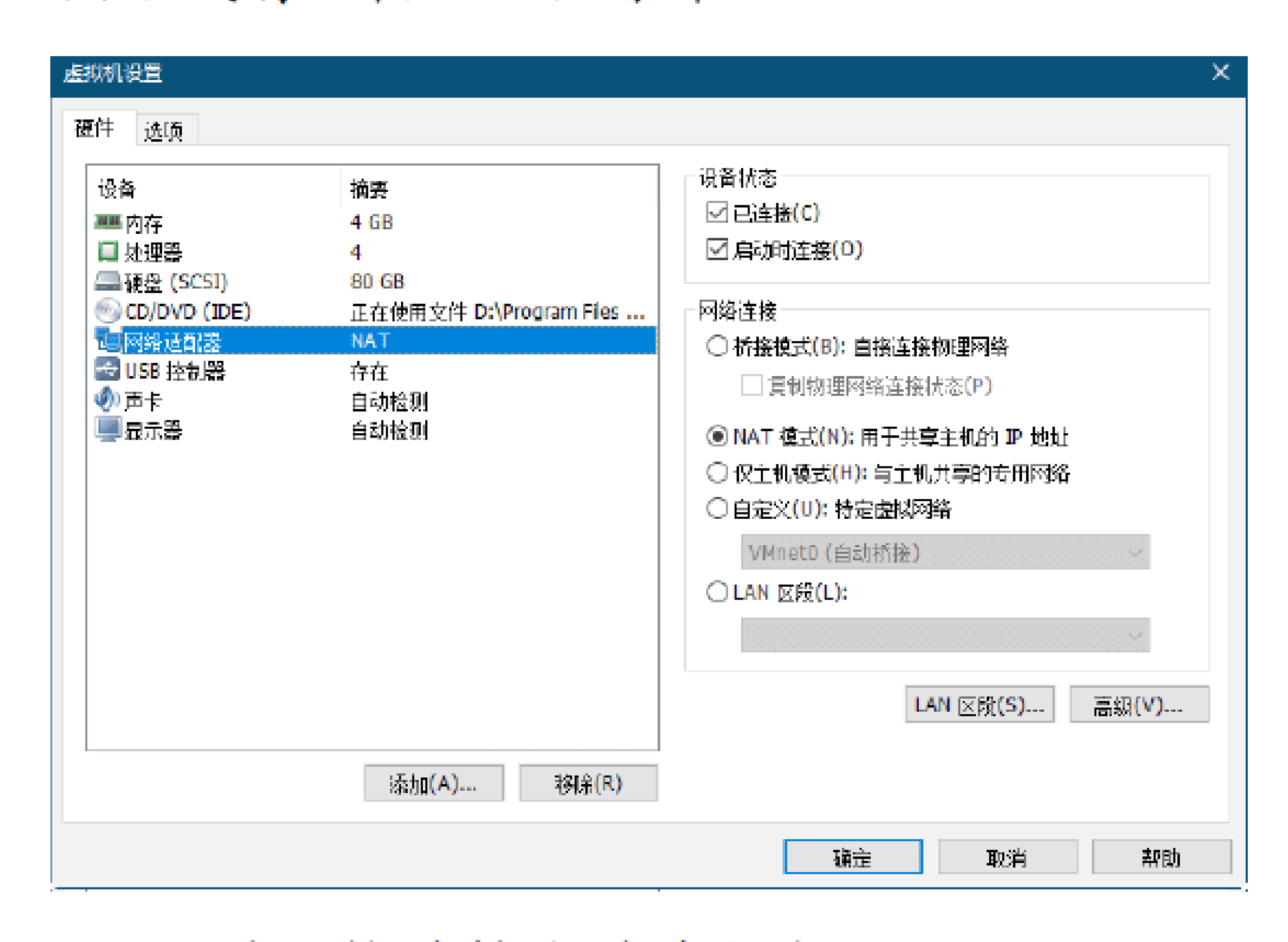
实战演练2——设置Kali虚拟机的上网方式

Kali虚拟机可以设置3种网络模式，设置上网方式的操作步骤如下。

Step 01 在VMware菜单项中，选择“虚拟机”→“可移动设备”→“网络适配器”→“设置”选项，如下图所示。



Step 02 打开“虚拟机设置”对话框，在其中选择“网络适配器”选项，在右侧可以看到“网络连接”设置界面，这里提供的连接方式有3种，如下图所示。



3种网络连接方式介绍如下：

（1）桥接模式：如果选择该连接模式，虚拟机可以获取独立的IP地址，通过独立IP地址进行上网。

（2）NAT模式：如果选择该连接模式，虚拟机将与主机共用一个IP地址，通过主机IP地址实现NAT转换上网。

（3）仅主机模式：如果选择该连接模式，虚拟机仅同主机进行通信，不能接入因特网外网。



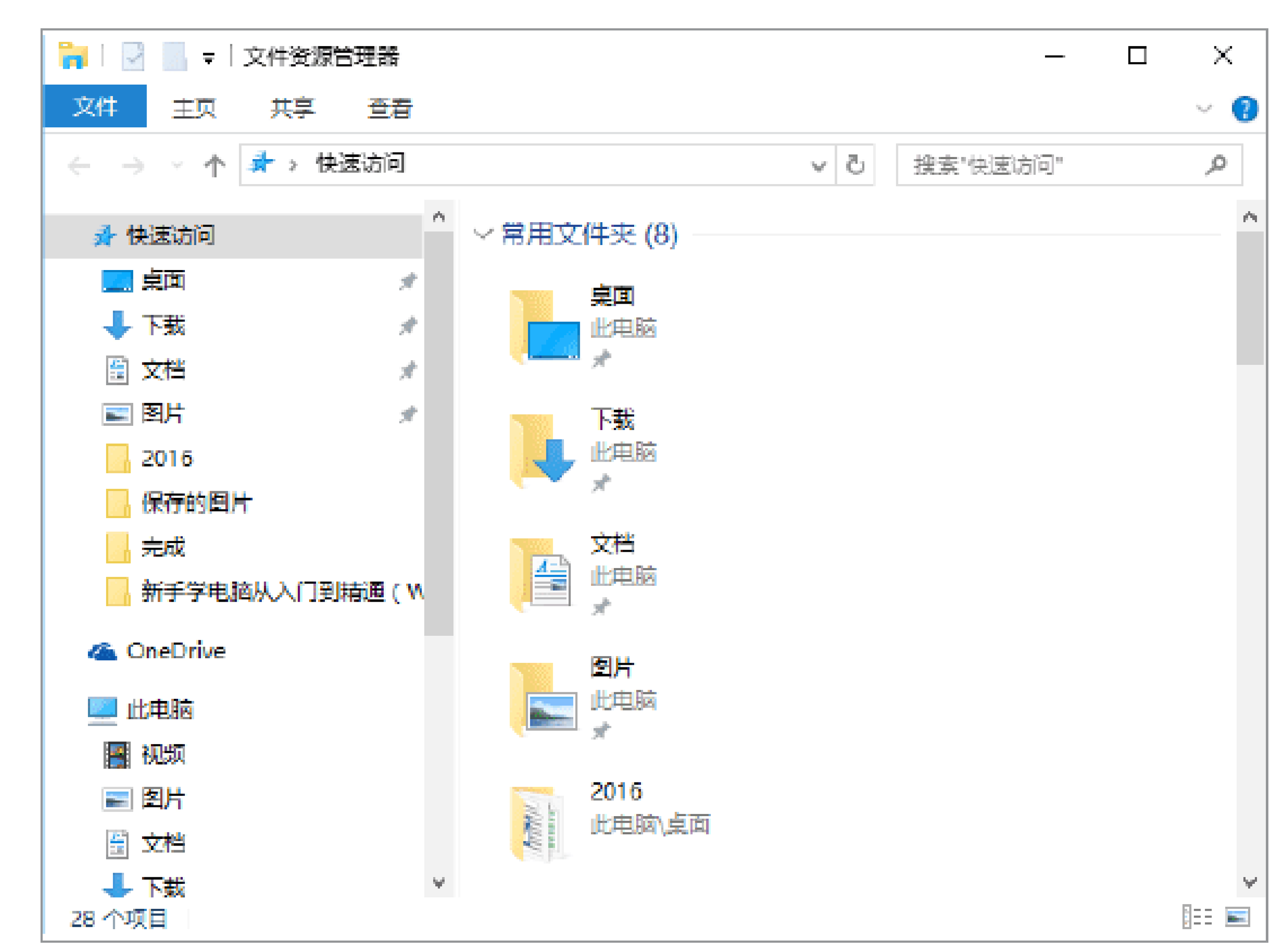
2.5 小试身手



练习1：显示系统文件的扩展名

Windows 10系统默认情况下并不显示文件的扩展名，用户可以通过设置显示文件的扩展名。具体操作步骤如下。

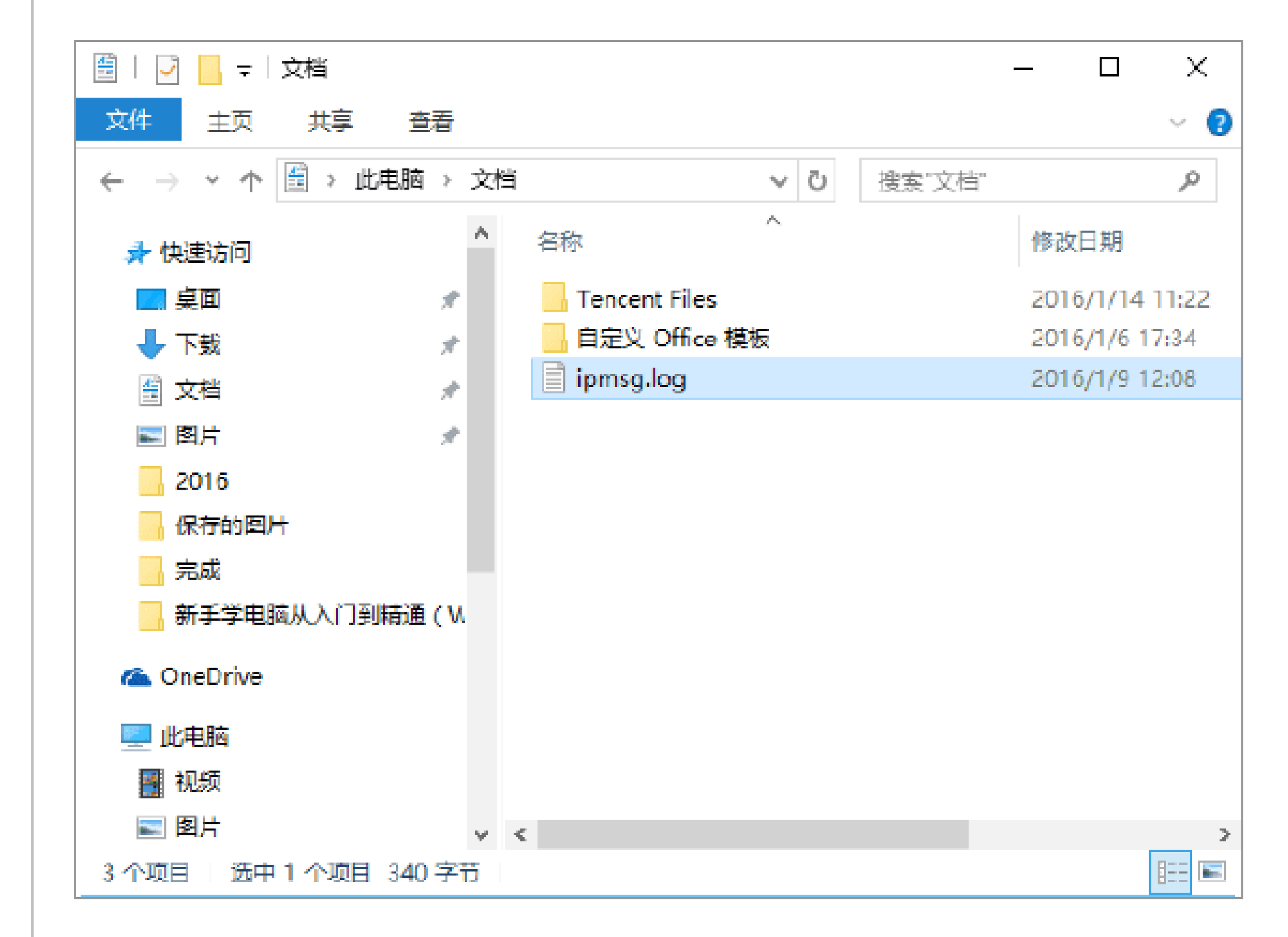
Step 01 单击“开始”按钮，在弹出的“开始”菜单中选择“文件资源管理器”选项，打开“文件资源管理器”窗口，如下图所示。



Step 02 选择“查看”选项卡，在打开的功能区域中勾选“显示/隐藏”区域中的“文件扩展名”复选框，如下图所示。



Step 03 此时打开一个文件夹，用户便可以查看文件的扩展名，如下图所示。

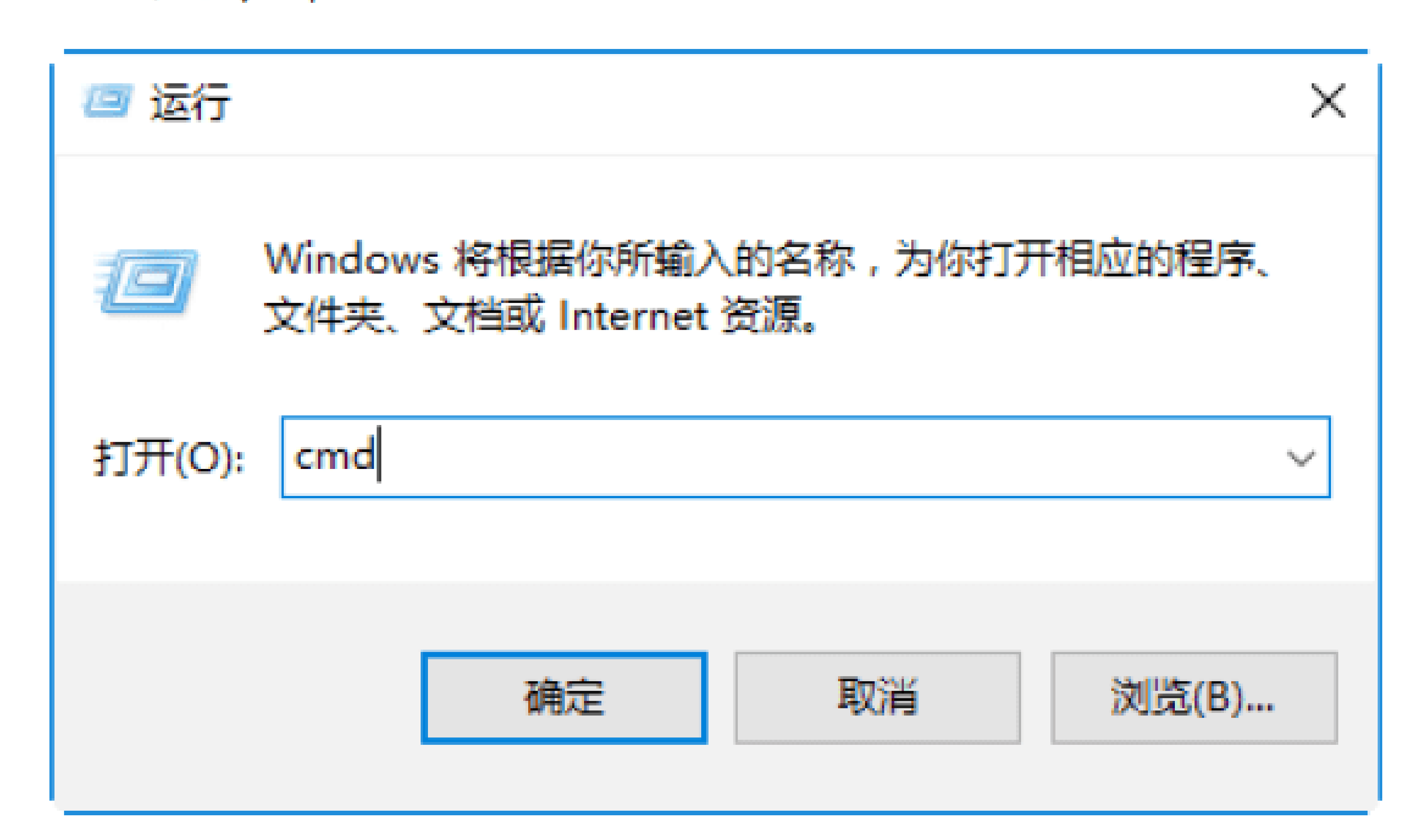


练习2：查看系统中的ARP缓存表

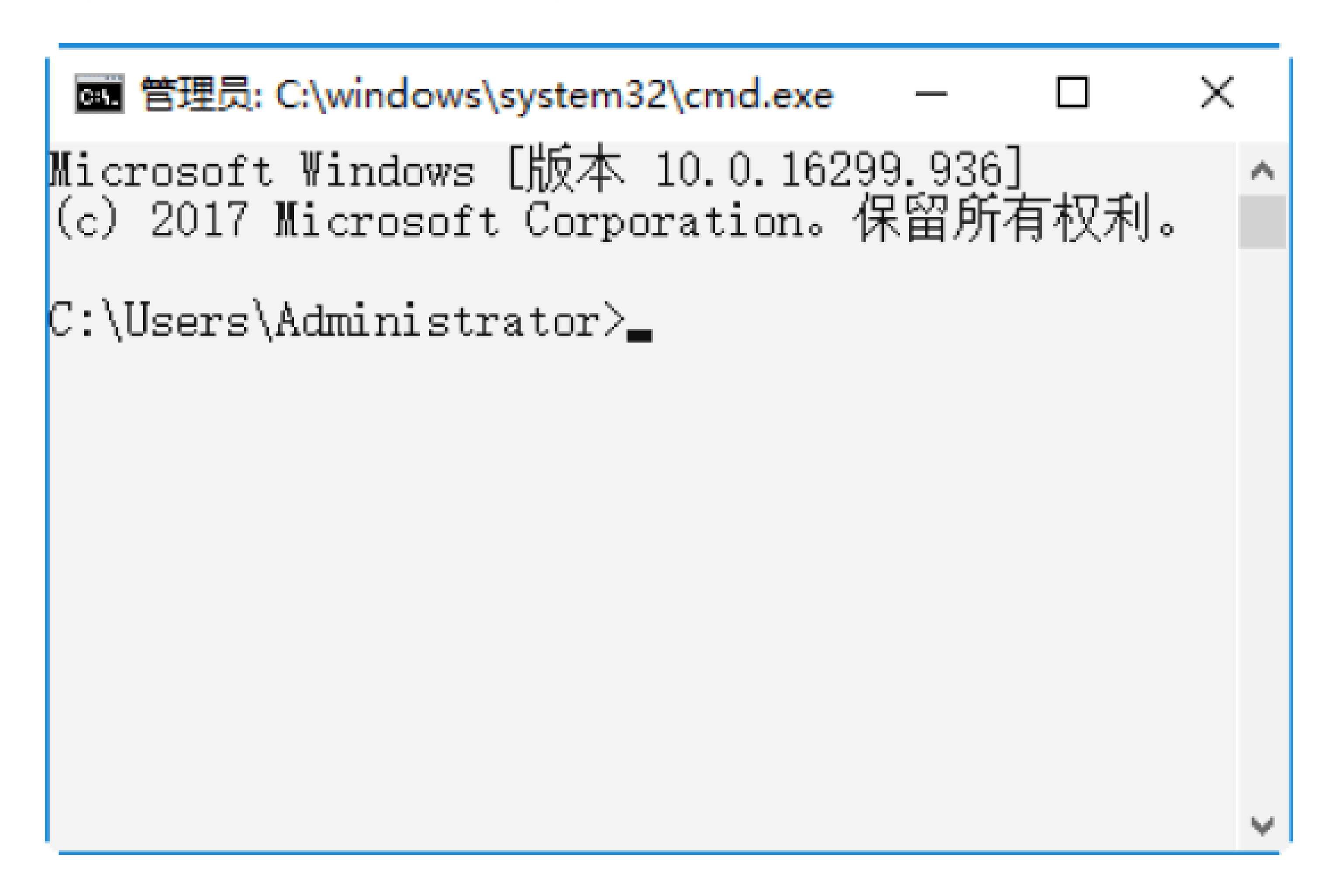
在利用网络欺骗攻击的过程中，经常用到的一种欺骗方式是ARP欺骗，但在实

施ARP欺骗之前，需要查看ARP缓存表。那么如何查看系统的ARP缓存表信息呢？具体的操作步骤如下。

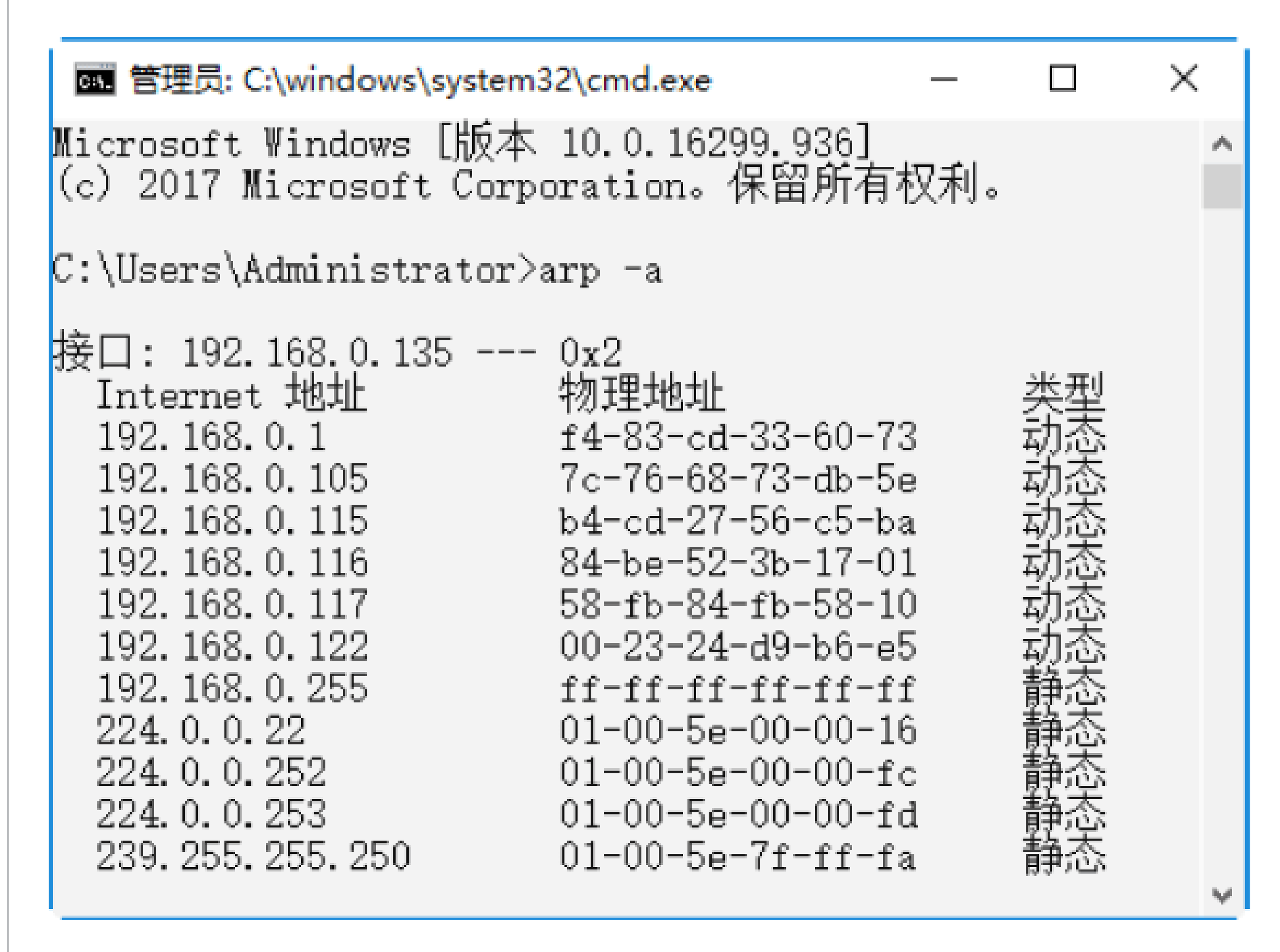
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“运行”选项，打开“运行”对话框，在“打开”文本框中输入cmd命令，如下图所示。



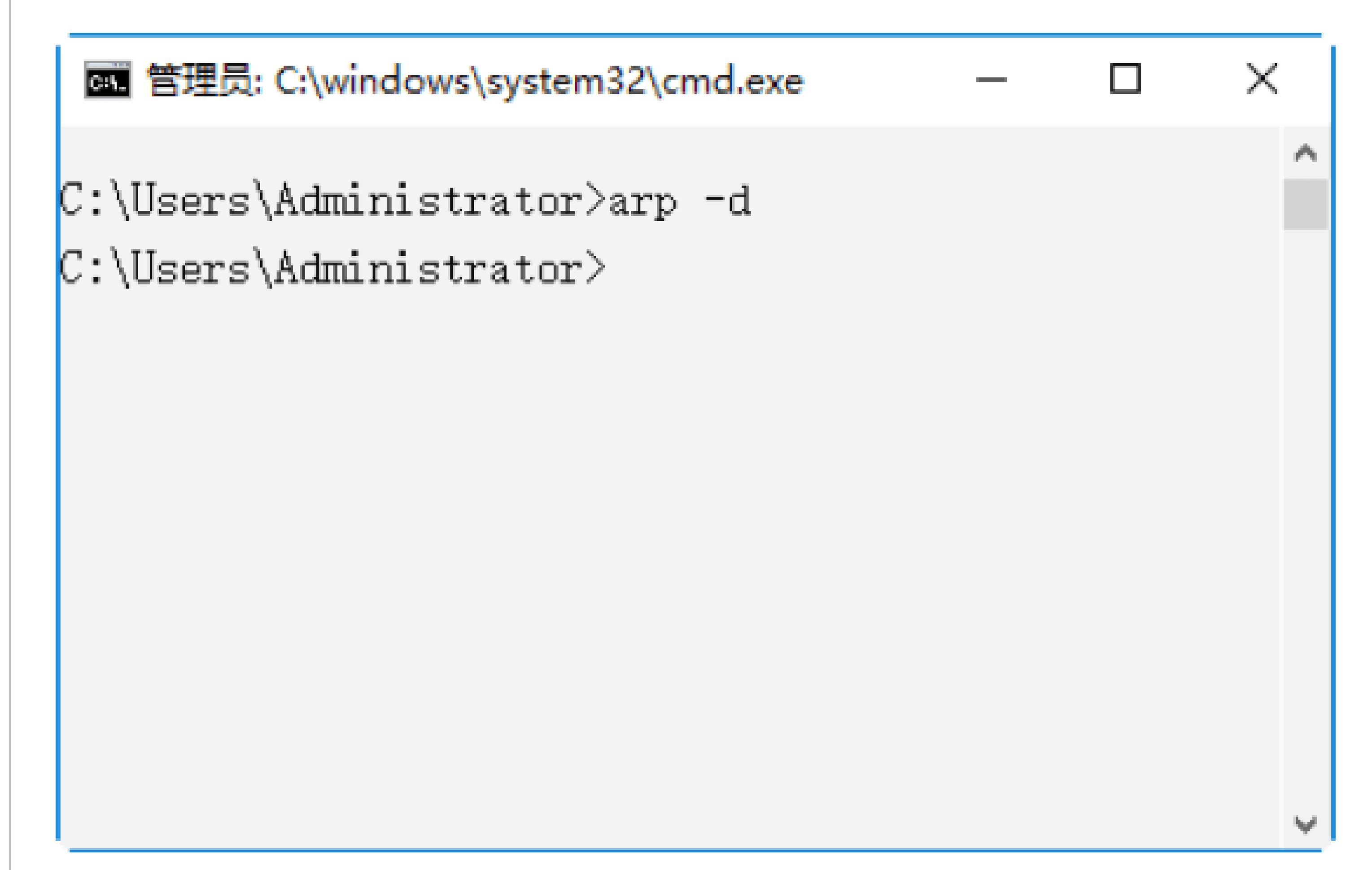
Step 02 单击“确定”按钮，打开“命令提示符”窗口，如下图所示。



Step 03 在“命令提示符”窗口中输入arp -a命令，按Enter键执行命令，即可显示出本机系统的ARP缓存表中的内容，如下图所示。



Step 04 在“命令提示符”窗口中输入arp -d命令，按Enter键执行命令，即可删除ARP缓存表中所有的内容，如下图所示。



第3章　黑客入侵方式与DOS命令

作为计算机或网络终端设备的用户，要想使自己的设备不受或少受黑客的攻击，就必须了解一些黑客常用的入侵方法以及常用的DOS命令。本章介绍黑客常用的入侵方式以及常用的DOS命令，主要包括cd命令、dir命令、ping命令等。

3.1　黑客常用入侵方式

在互联网中，为了防止黑客入侵自己的计算机，就必须了解黑客入侵目标计算机的常用方法。黑客常用的入侵方法有获取口令入侵、远程控制入侵、木马病毒入侵、系统漏洞入侵、电子邮件入侵、网络监听入侵等。

3.1.1　获取口令入侵

口令入侵是黑客常用的入侵网络的方法。黑客通过获取系统管理员或其他用户的口令，进而获得系统的管理权，从而窃取系统信息、磁盘中的文件甚至对系统进行破坏。获取口令入侵的3种方法如下：

（1）通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大，监听者往往能够获得其所在网段的所有用户账号和口令，对局域网安全威胁比较大。

（2）在知道用户的账号后，如电子邮件@前面的部分，利用一些密码破解工具强行破解用户口令，这种方法不受网段限制，但黑客要有足够的耐心和时间。

（3）在获得一个服务器上的用户口令文件（此文件为Shadow文件）后，用暴力破解程序破解用户口令。该方法的使用前提是黑客已经获得带有口令的Shadow文件。此方法在所有方法中危害最大，因为它不需要像第（2）种方法那样一遍又一遍地尝试登录服务器，而是在本地将加密后的口令与Shadow文件中的口令相比较就能非常容易地破获用户密码。尤其对那些将口令安全系数设置极低的用户，如某用户账号为lty，其口令就是lty666、666666，或干脆就是lty等，更是在短短的一两分钟内，甚至几十秒内就可以将其破解。

3.1.2　远程控制入侵

远程控制是在网络上由一台计算机（主控端/客户端）远距离去控制另一台计算机（被控端/服务器端）的技术，而远程一般是指通过网络控制远端计算机。通过远程控制入侵方法，可以获取目标主机的如下内容：

（1）获取目标计算机屏幕图像、窗口及进程列表；

（2）记录并提取远端键盘事件；

（3）打开、关闭目标计算机的任意目录并实现资源共享；

（4）激活、终止远端程序进程；

（5）管理远端计算机的文件和文件夹；

（6）关闭或者重新启动远端计算机中的操作系统；

（7）修改Windows注册表；

（8）在远端计算机上进行下载文件和捕获音频、视频信号等多种操作。

远程控制一般支持LAN、WAN、拨号、互联网等网络方式。此外，有的远程控制软件还支持通过串口、并口等方式对远程主机进行控制。随着网络技术的发展，目前很多远程控制软件提供通过Web页面，以Java技术来控制远程计算机，这样可以实现不同操作系统下的远程控制。

3.1.3　木马病毒入侵

木马病毒程序可以直接侵入用户的计算机并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有木马病毒程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，这些木马病毒程序就会留在用户的计算机中，并在用户的计算机系统中隐藏，当Windows启动时，这些木马病毒便被悄悄执行。

当用户将自己的计算机连接到因特网，这个木马病毒程序就会通知黑客，报告用户的IP地址以及预先设定的端口。黑客在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改用户的计算机参数设定，复制文件，窥视用户整个硬盘中的内容等，从而达到控制用户计算机的目的。

3.1.4　系统漏洞入侵

目前，大多数计算机安装的是Windows操作系统，虽然Windows操作系统的稳定性和安全性随着其版本的提升而得到不断的提高，但仍然会出现不同的安全隐患，即漏洞。

黑客可以利用专业的工具发现这些漏洞，在了解目标计算机存在的漏洞和缺点后，黑客就可以利用缓冲区溢出和测试用户的账户和密码等方式，来实现对该主机进行试探性攻击的目的。

3.1.5　电子邮件入侵

电子邮件入侵主要表现为两种方式，具体介绍如下：

一是电子邮件轰炸。也就是通常所说的邮件炸弹，指的是用伪造的IP地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪。

二是电子邮件欺骗。攻击者可以假称自己为系统管理员，给用户发送邮件要求用户修改口令或在貌似正常的附件中加载病毒或其他木马程序，这类欺骗只要用户提高警惕，一般危害性不是太大。

3.1.6　网络监听入侵

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。此时，如果两台主机进行通信的信息没有加密，只要使用网络监听工具，如SpyNet Sniffer、SRSniffer等，就可以轻而易举地截取包括口令和账号在内的信息。

3.2　黑客常用DOS命令实战

熟练掌握一些DOS命令的应用是一名黑客的基本功，通过这些DOS命令可以帮助计算机用户追踪黑客的踪迹。

实战1：切换当前目录的cd命令

使用cd（Change Directory）命令可以改变当前目录，该命令用于切换路径目录。cd命令主要有以下3种使用方法。

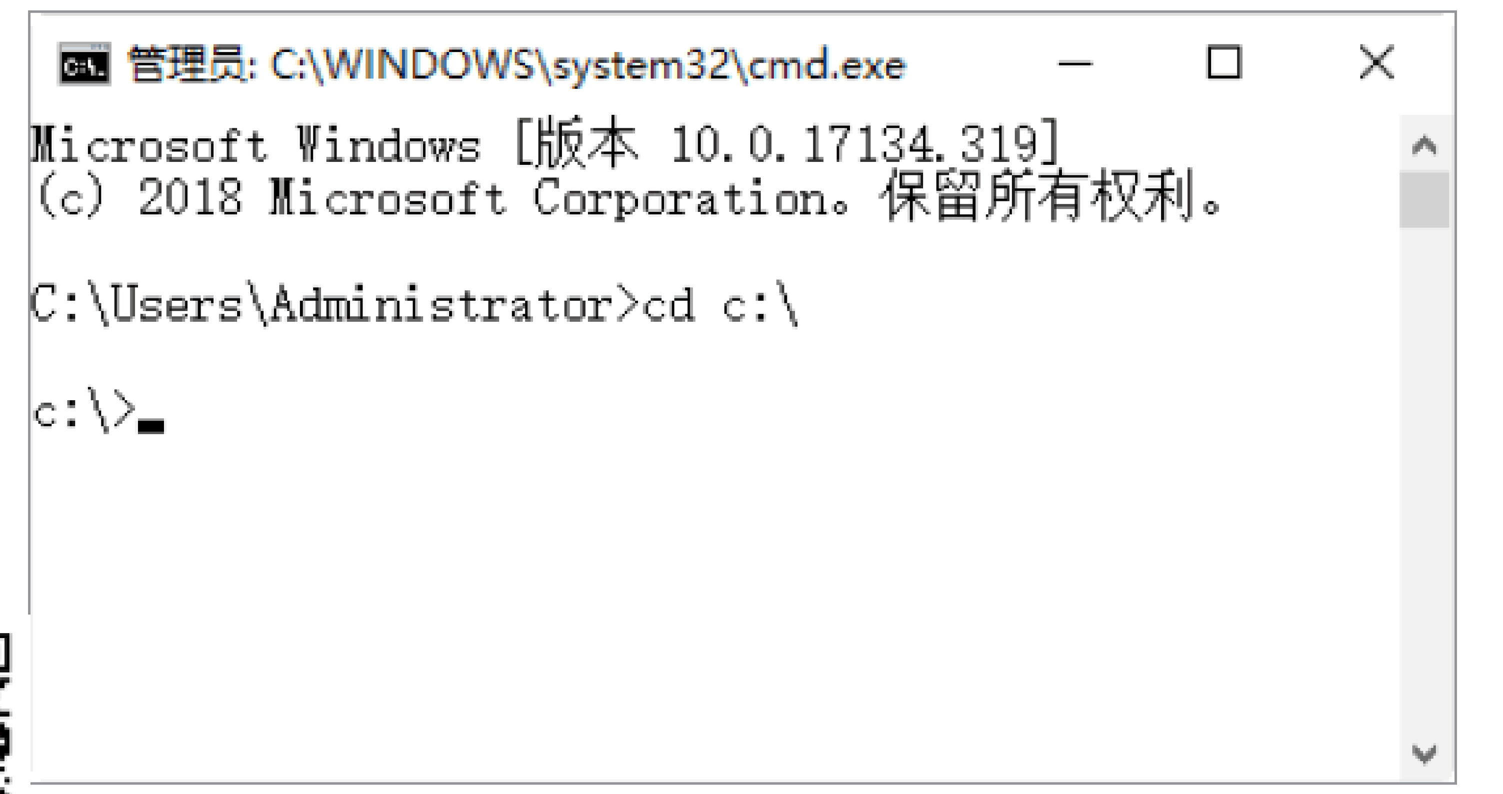
（1）cd path：path是路径。例如，输入cd C:\命令后按Enter键，或输入cd Windows命令，即可分别切换到C:\和C:\Windows目录下。

（2）cd..：cd后面的两个“.”表示返回上一级目录。例如，当前的目录为C:\Windows，如果输入cd..命令，按Enter键即可返回上一级目录，即C:\。

（3）cd\：表示当前无论在哪个子目录下，通过该命令可立即返回到根目录下。例如，使用cd命令进入C:\Windows\system32子目录，并退回根目录。具体操作步骤如下。



Step 01 在“命令提示符”窗口中输入cd c:\命令，按Enter键，即可将目录切换为C:\，如下图所示。

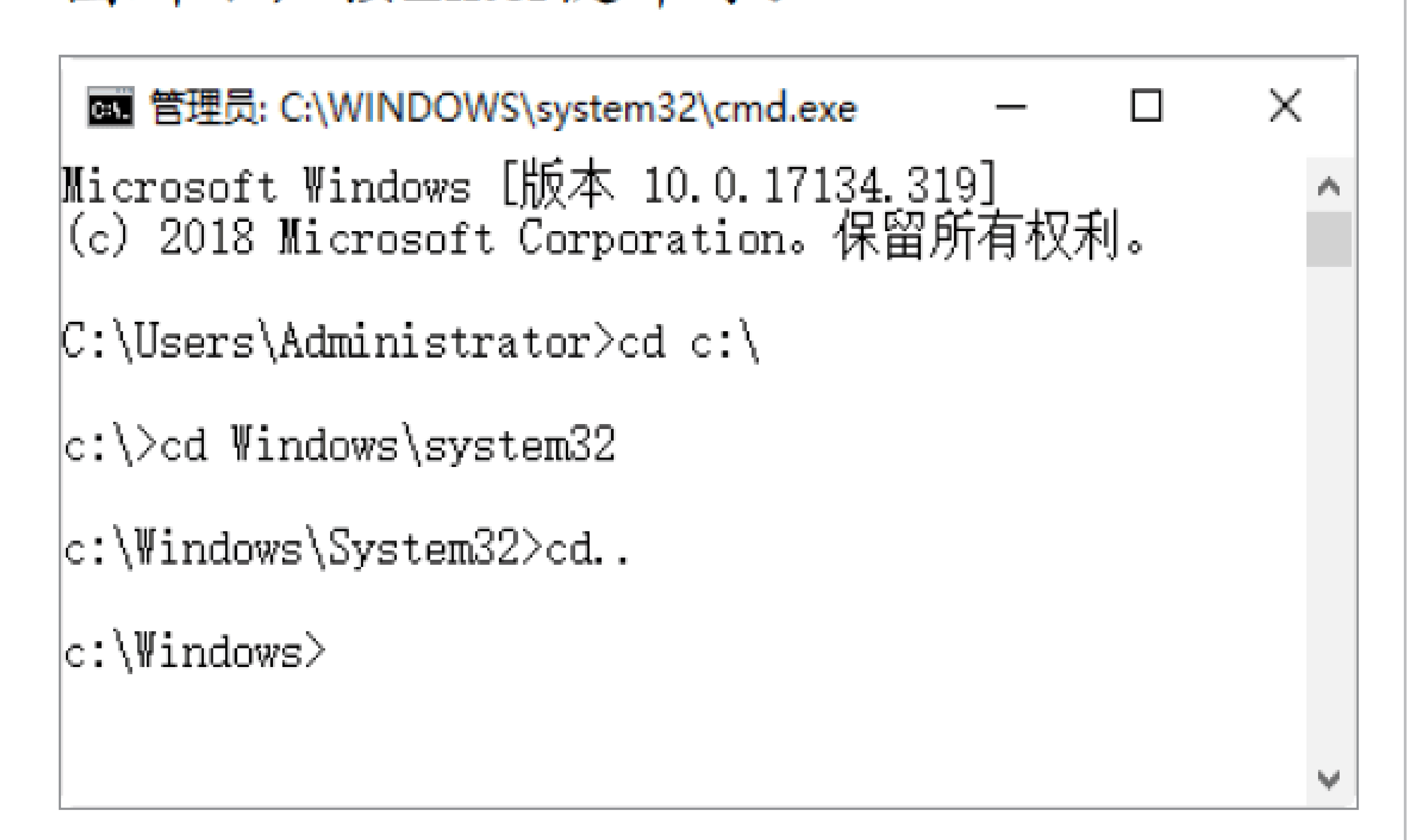




Step 02 如果想进入C:\Windows\system32目录中，则需在上面的“命令提示符”窗口中输入cd Windows\system32命令，按Enter键，即可将目录切换为C:\Windows\system32，如下图所示。



Step 03 如果想返回上一级目录，则可以在“命令提示符”窗口中输入cd..命令，如下图所示，按Enter键即可。



Step 04 如果想返回到根目录，则可以在“命令提示符”窗口中输入cd\命令，如下图所示，按Enter键即可。



实战2：列出磁盘目录文件的dir命令

使用dir命令可以列出磁盘上所有的或指定的文件目录，主要显示的内容包含卷标、文件名、文件大小、文件建立日期和时间、目录名、磁盘剩余空间等。dir命令的语法格式如下：

```
dir [盘符][路径][文件名][/P][/W][/A:属性]
```

其中，各个参数的作用如下。

（1）/P：当显示的信息超过一屏时暂停显示，直至按任意键才继续显示。

（2）/W：以横向排列的形式显示文件名和目录名，每行5个（不显示文件大小、建立日期和时间）。

（3）/A:属性：仅显示指定属性的文件，无此参数时，dir显示除系统和隐含文件外的所有文件。可指定为以下几种形式：

① /AS：显示系统文件的信息；

② /AH：显示隐含文件的信息；

③ /AR：显示只读文件的信息；

④ /AA：显示归档文件的信息；

⑤ /AD：显示目录信息。

例如，使用dir命令查看磁盘中文件信息的具体操作步骤如下。

Step 01 在“命令提示符”窗口中输入dir命令，按Enter键，即可查看当前目录下的文件列表，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.17134.319]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>dir
 驱动器 C 中的卷是 Windows
 卷的序列号是 2ECC-1807

 C:\Users\Administrator 的目录

2018/11/26  12:43    <DIR>          .
2018/11/26  12:43    <DIR>          ..
2018/11/26  12:43    <DIR>          3D Objects
2018/11/26  12:43    <DIR>          Contacts
2018/11/26  12:47    <DIR>          Desktop
2018/11/26  12:43    <DIR>          Documents
2018/11/26  12:43    <DIR>          Downloads
2018/11/26  12:43    <DIR>          Favorites
2018/11/26  12:43    <DIR>          Links
2018/11/26  12:43    <DIR>          Music
2018/09/19  12:45    <DIR>          OneDrive
2018/11/26  12:43    <DIR>          Pictures
2016/11/28  11:11    <DIR>          Roaming
2018/11/26  12:43    <DIR>          Saved Games
2018/11/26  12:43    <DIR>          Searches
2018/11/26  12:43    <DIR>          Videos
               0 个文件              0 字节
              16 个目录 28,804,747,264 可用字节

C:\Users\Administrator>
```

Step 02 在“命令提示符”窗口中输入dir d:/ a:d命令，按Enter键，即可查看D盘下的所有文件的目录，如下图所示。

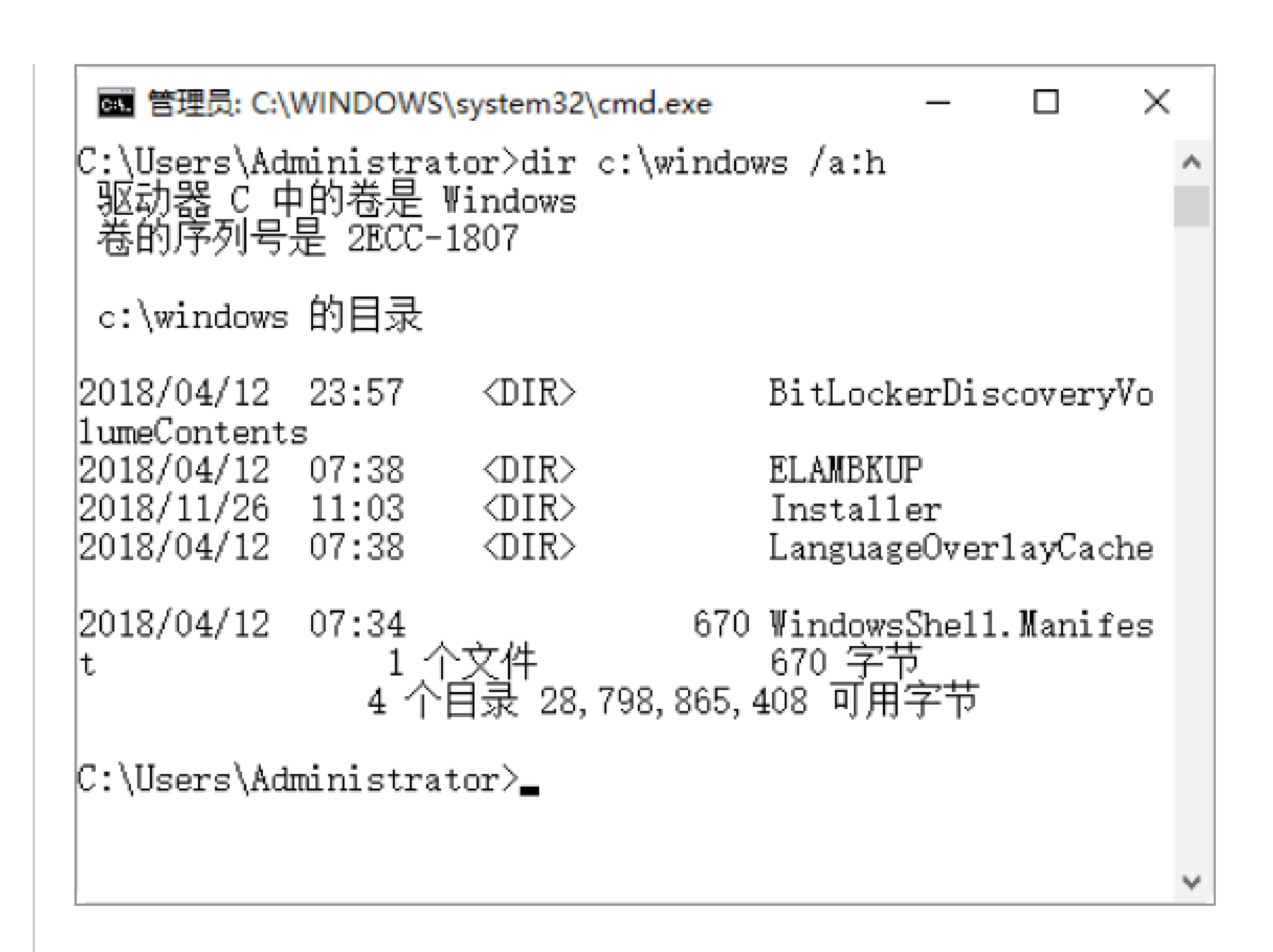
```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>dir d:/ a:d
 驱动器 D 中的卷是 软件
 卷的序列号是 B0CE-3B52

 D:\ 的目录

2017/02/13  13:45    <DIR>          $RECYCLE.BIN
2017/07/31  16:22    <DIR>          -c-a-d2016注册
2018/07/05  18:32    <DIR>          1
2018/11/20  19:03    <DIR>          2
2017/07/21  17:28    <DIR>          360Downloads
2018/11/20  18:50    <DIR>          360安全浏览器下载
2017/07/31  18:33    <DIR>          3Dmax
2017/07/25  09:45    <DIR>          Adobe CC 2015 通用破
解补丁v1.5
2015/06/24  08:53    <DIR>          AdobeCC20142015pj
2017/11/14  18:27    <DIR>          AdobeDreamweaverCS6
2017/02/11  14:34    <DIR>          AutoCAD_2016_Simplifi
ed_Chinese_Win_64bit_dlm
2017/02/19  19:45    <DIR>          CamtasiaStudio-v6.03H

2017/03/01  19:40    <DIR>          DESKTOP-RJKNMOC
2017/03/03  11:27    <DIR>          HyperSnap 6
2017/08/02  18:02    <DIR>          Java
2018/09/21  13:07    <DIR>          js
2018/11/20  18:57    <DIR>          my
2017/08/03  10:33    <DIR>          MyDrivers
2017/03/23  11:57    <DIR>          Office2016_zh_32Bit
2017/11/10  12:40    <DIR>          office2016正式版激活
```

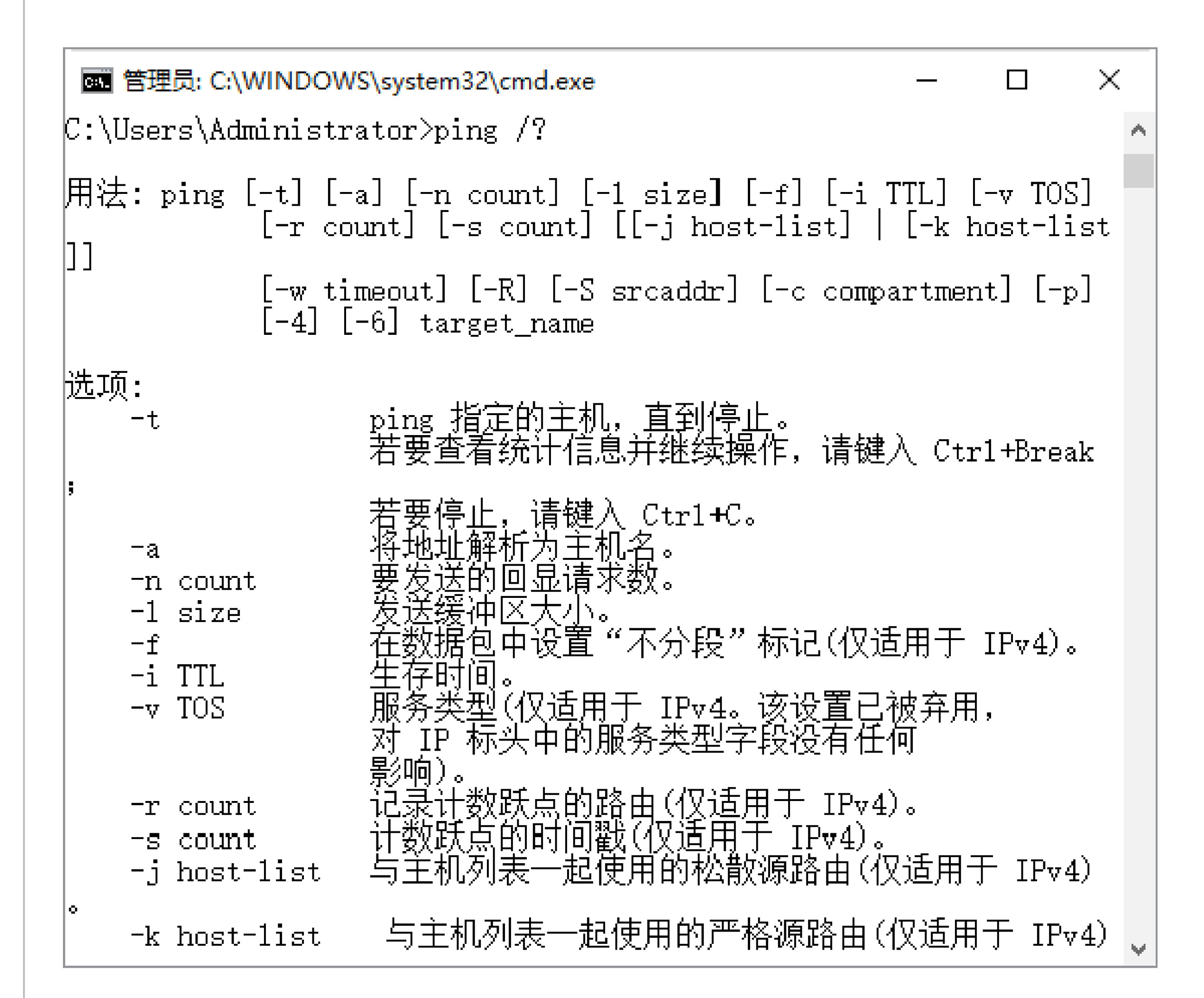
Step 03 在“命令提示符”窗口中输入dir c:\windows /a:h命令，按Enter键，即可列出c:\windows目录下的隐藏文件，如下图所示。



实战3：检查计算机连接状态的ping命令



ping命令是TCP/IP中最为常用的命令之一，主要用来检查网络是否通畅或者网络连接的速度。对于一个黑客来说，ping命令是第一个必须掌握的DOS命令。在“命令提示符”窗口中输入ping /?，可以得到命令的帮助信息，如下图所示。



使用ping命令对计算机的连接状态进行测试的具体操作步骤如下。

Step 01 使用ping命令判断计算机的操作系统类型。在“命令提示符”窗口中输入ping 192.168.0.130命令，运行结果如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>ping 192.168.0.130

正在 ping 192.168.0.130 具有 32 字节的数据:
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128

192.168.0.130 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失)
,
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>
```

Step 02 在“命令提示符”窗口中输入ping 192.168.0.130 –t –l 128命令，可以不断向某台主机发出大量的数据包，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe - ping ...
C:\Users\Administrator>ping 192.168.0.130 -t -l 128

正在 ping 192.168.0.130 具有 128 字节的数据:
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=128 时间<1ms TTL=128
```



Step 03 判断本台计算机是否与外界网络连通。在“命令提示符”窗口中输入ping www.baidu.com命令，其运行结果如下图所示，说明本台计算机与外界网络连通。

```
管理员: C:\WINDOWS\system32\cmd.exe
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping www.baidu.com

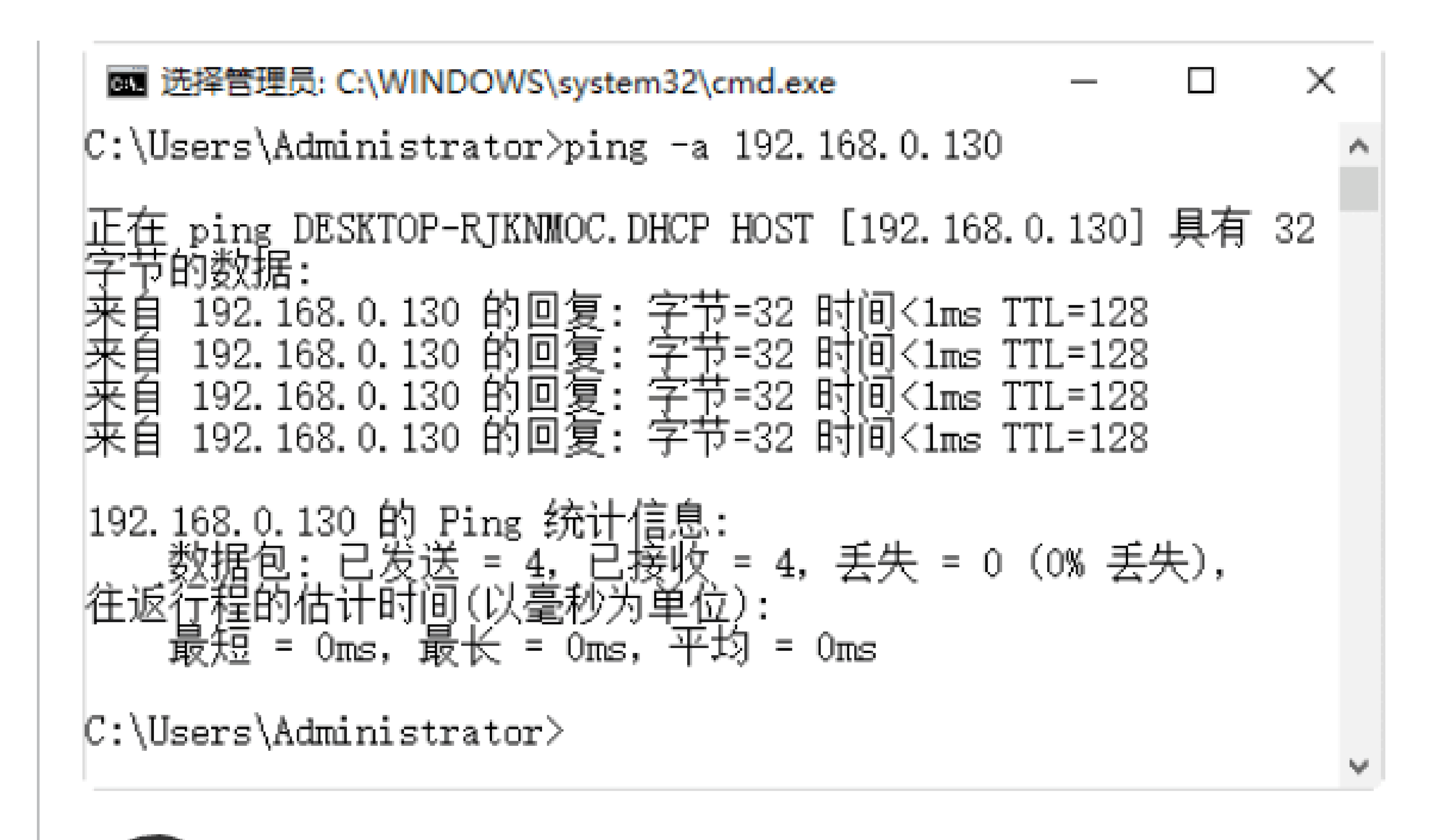
正在 Ping www.wshifen.com [103.235.46.39] 具有 32 字节的数据:

来自 103.235.46.39 的回复: 字节=32 时间=285ms TTL=45
来自 103.235.46.39 的回复: 字节=32 时间=279ms TTL=45
来自 103.235.46.39 的回复: 字节=32 时间=300ms TTL=45
来自 103.235.46.39 的回复: 字节=32 时间=352ms TTL=45

103.235.46.39 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 279ms, 最长 = 352ms, 平均 = 304ms

C:\Users\Administrator>_
```

Step 04 解析某IP地址的计算机名。在“命令提示符”窗口中输入ping -a 192.168.0.130命令，其运行结果如下图所示，可知这台主机的名称为DESKTOP-RJKNMOC。



```
选择管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>ping -a 192.168.0.130

正在 ping DESKTOP-RJKNMOC.DHCP HOST [192.168.0.130] 具有 32 字节的数据:
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.0.130 的回复: 字节=32 时间<1ms TTL=128

192.168.0.130 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Administrator>
```

知识链接

利用TTL（Time To Live，生存时间）值判断操作系统类型。由于不同的操作系统的主机设置的TTL值是不同的，所以可以根据其中TTL值来识别操作系统类型。一般情况下，分以下3种：

（1）TTL=32，则认为目标主机操作系统为Windows 95/98。

（2）TTL=64～128，则认为目标主机操作系统为Windows NT/2000/XP/7/10。

（3）TTL=128～255或者32～64，则认为是UNIX/Linux操作系统。

实战4：查询网络状态与共享资源的net命令

使用net命令可以查询网络状态、共享资源以及计算机所开启的服务等，该命令的语法格式如下。

```
net [ accounts | computer | config | continue | file | group | help | helpmsg | localgroup | name | pause | print | send | session | share | start | statistics | stop | time | use | user | view ]
```

查询本台计算机开启哪些Window服务的具体操作步骤如下。

Step 01 使用net命令查看网络状态。打开“命令提示符”窗口，输入net start命令，如下图所示。

```
管理员: C:\WINDOWS\system32\cm...
Microsoft Windows [版本 10.0.17134.319]
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>net start_
```

Step 02 按Enter键，则在打开的“命令提示符”窗口中可以显示计算机所启动的Windows服务，如下图所示。


```
管理员: C:\WINDOWS\system32\cmd.exe
(c) 2018 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>net start
已经启动以下 Windows 服务:

   Application Information
   AVCTP 服务
   Background Intelligent Transfer Service
   Background Tasks Infrastructure Service
   Base Filtering Engine
   BrYNSvc
   Certificate Propagation
   Client License Service (ClipSVC)
   CNG Key Isolation
   COM+ Event System
   Computer Browser
   Connected User Experiences and Telemetry
   Contact Data_1f8b75a4
   CoreMessaging
   Credential Manager
   Cryptographic Services
   Data Sharing Service
   DCOM Server Process Launcher
   Delivery Optimization
   Device Association Service
   DHCP Client
```

实战5：显示网络连接信息的netstat命令

netstat命令主要用来显示网络连接的信息，包括显示活动的TCP连接、路由器和网络接口信息，是一个监控TCP/IP网络非常有用的工具，可以让用户得知系统中目前都有哪些网络连接正常。

在“命令提示符”窗口中输入netstat/?命令，可以得到这条命令的帮助信息。

```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>netstat/?

显示协议统计信息和当前 TCP/IP 网络连接。

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-x] [-t] [in
terval]

  -a            显示所有连接和侦听端口。
  -b            显示在创建每个连接或侦听端口时涉及的
                可执行程序。在某些情况下，已知可执行程序承载
                多个独立的组件，这些情况下，
                显示创建连接或侦听端口时
                涉及的组件序列。在此情况下，可执行程序的
                名称位于底部 [] 中，它调用的组件位于顶部，
                直至达到 TCP/IP。注意，此选项
                可能很耗时，并且在你没有足够
                权限时可能失败。
  -e            显示以太网统计信息。此选项可以与 -s 选项
                结合使用。
  -f            显示外部地址的完全限定
                域名(FQDN)。
  -n            以数字形式显示地址和端口号。
  -o            显示拥有的与每个连接关联的进程 ID。
  -p proto      显示 proto 指定的协议的连接；proto
                可以是下列任何一个: TCP、UDP、TCPv6 或 UDPv6。如果与 -s
                选项一起用来显示每个协议的统计信息，proto 可以是下列任何
一个:
```

该命令的语法格式如下：

```
netstat [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]
```

其中，比较重要的参数的含义如下。

（1）-a：显示所有连接和监听端口。

（2）-n：以数字形式显示地址和端口号。

使用netstat命令查看网络连接的具体操作步骤如下。

Step 01 打开“命令提示符”窗口，在其中输入netstat -n或netstat命令，按Enter键，即可查看服务器活动的TCP/IP连接，如下图所示。


```
管理员: C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>netstat

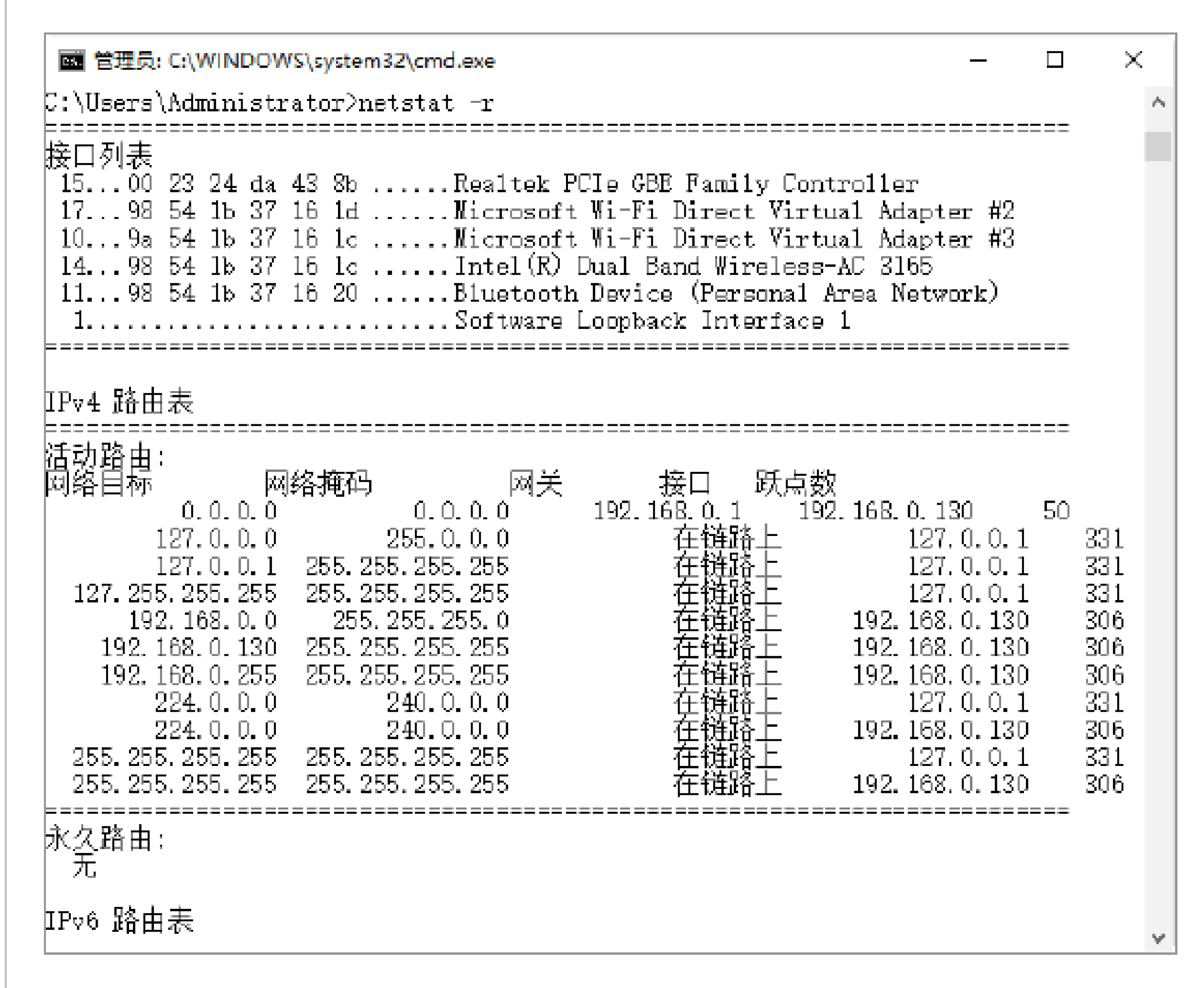
活动连接

  协议  本地地址              外部地址              状态
  TCP    127.0.0.1:1521         DESKTOP-RJKNMOC:49700  ESTABLISHED
  TCP    127.0.0.1:1521         DESKTOP-RJKNMOC:49702  ESTABLISHED
  TCP    127.0.0.1:49700        DESKTOP-RJKNMOC:1521   ESTABLISHED
  TCP    127.0.0.1:49702        DESKTOP-RJKNMOC:1521   ESTABLISHED
  TCP    192.168.0.130:50224    a104-124-190-57:https  ESTABLISHED
  TCP    192.168.0.130:50665    123.151.79.44:https    CLOSE_WAIT
  TCP    192.168.0.130:51279    52.230.3.194:https     ESTABLISHED
  TCP    192.168.0.130:51556    111.206.57.247:http    ESTABLISHED
  TCP    192.168.0.130:52126    125.74.5.166:http      CLOSE_WAIT
  TCP    192.168.0.130:52204    hn:http                ESTABLISHED
  TCP    192.168.0.130:52418    36.99.30.169:http      ESTABLISHED
  TCP    192.168.0.130:52428    180.163.238.167:https  ESTABLISHED
  TCP    192.168.0.130:52432    52.229.207.60:https    ESTABLISHED
  TCP    192.168.0.130:52433    203.208.39.104:http    SYN_SENT

C:\Users\Administrator>
```



Step 02 在“命令提示符”窗口中输入netstat -r命令，按Enter键，即可查看本机的路由信息，如下图所示。


```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>netstat -r
===========================================================================
接口列表
 15...00 23 24 da 43 8b ......Realtek PCIe GBE Family Controller
 17...98 54 1b 37 16 1d ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...9a 54 1b 37 16 1c ......Microsoft Wi-Fi Direct Virtual Adapter #3
 14...98 54 1b 37 16 1c ......Intel(R) Dual Band Wireless-AC 3165
 11...98 54 1b 37 16 20 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.130     50
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1    331
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1    331
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
      192.168.0.0    255.255.255.0            在链路上     192.168.0.130    306
    192.168.0.130  255.255.255.255            在链路上     192.168.0.130    306
    192.168.0.255  255.255.255.255            在链路上     192.168.0.130    306
        224.0.0.0        240.0.0.0            在链路上         127.0.0.1    331
        224.0.0.0        240.0.0.0            在链路上     192.168.0.130    306
  255.255.255.255  255.255.255.255            在链路上         127.0.0.1    331
  255.255.255.255  255.255.255.255            在链路上     192.168.0.130    306
===========================================================================
永久路由:
  无

IPv6 路由表
```

Step 03 在“命令提示符”窗口中输入netstat -a命令，按Enter键，即可查看本机所有活动的TCP连接，如下图所示。



```
管理员: C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>netstat -a

活动连接

  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:3308           DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:5501           DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:7680           DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:11000          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:11010          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:11020          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49674          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49699          DESKTOP-RJKNMOC:0      LISTENING
  TCP    0.0.0.0:49701          DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:1434         DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:1521         DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:1521         DESKTOP-RJKNMOC:49700  ESTABLISHED
  TCP    127.0.0.1:1521         DESKTOP-RJKNMOC:49702  ESTABLISHED
  TCP    127.0.0.1:4300         DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:4301         DESKTOP-RJKNMOC:0      LISTENING
  TCP    127.0.0.1:12101        DESKTOP-RJKNMOC:0      LISTENING
```

Step 04 在“命令提示符”窗口中输入netstat -n -a命令，按Enter键，即可显示本机所有连接的端口及其状态，如下图所示。

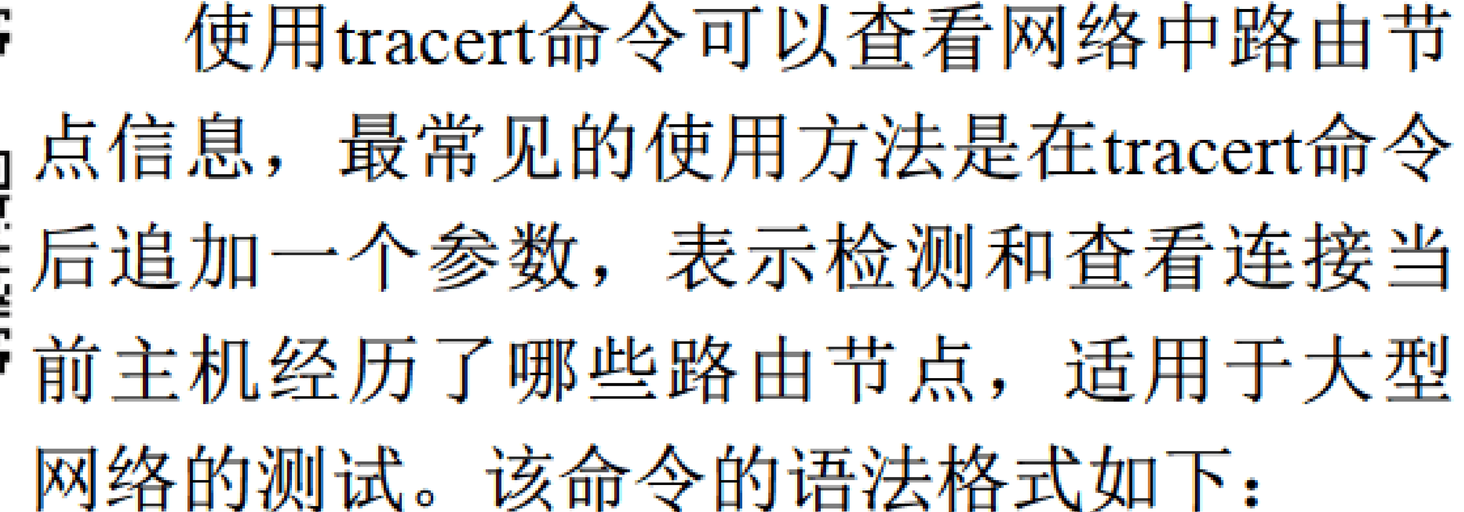
```
管理员: C:\WINDOWS\system32\cmd.exe
C:\Users\Administrator>netstat -n -a

活动连接

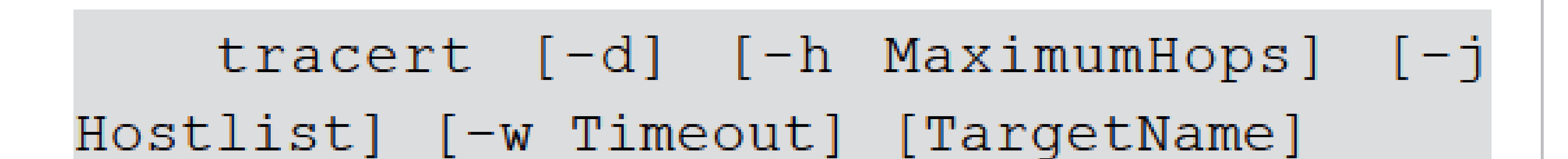
  协议  本地地址          外部地址        状态
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3308           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5501           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11000          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11010          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:11020          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49674          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49699          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49701          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1434         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1521         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1521         127.0.0.1:49700        ESTABLISHED
  TCP    127.0.0.1:1521         127.0.0.1:49702        ESTABLISHED
  TCP    127.0.0.1:4300         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:4301         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:12101        0.0.0.0:0              LISTENING
  TCP    127.0.0.1:31752        0.0.0.0:0              LISTENING
```



实战6：检查网络路由节点的tracert命令



使用tracert命令可以查看网络中路由节点信息，最常见的使用方法是在tracert命令后追加一个参数，表示检测和查看连接当前主机经历了哪些路由节点，适用于大型网络的测试。该命令的语法格式如下：



```
tracert [-d] [-h MaximumHops] [-j Hostlist] [-w Timeout] [TargetName]
```

其中，各个参数的含义如下。

（1）-d：防止解析目标主机的名字，可以加速显示tracert命令结果。

（2）-h MaximumHops：指定搜索到目标地址的最大跳跃数，默认为30个跳跃点。

（3）-j Hostlist：按照主机列表中的地址释放源路由。

（4）-w Timeout：指定超时时间间隔，默认单位为毫秒。

（5）TargetName：指定目标计算机。

例如，如果想查看www.baidu.com的路由与局域网络连接情况，则在“命令提示符”窗口中输入tracert www.baidu.com命令，按Enter键，其显示结果如下图所示。



```
管理员: C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>tracert www.baidu.com

通过最多 30 个跃点跟踪
到 www.wshifen.com [103.235.46.39] 的路由:

  1     1 ms     1 ms     5 ms  192.168.0.1
  2    12 ms     9 ms    38 ms  172.16.0.1
  3    22 ms     5 ms     *     222.83.34.105
  4     8 ms    10 ms     9 ms  222.83.40.161
  5   114 ms    77 ms   136 ms  202.97.38.133
  6    53 ms     *       56 ms  202.97.18.206
  7   149 ms   150 ms   146 ms  202.97.14.254
  8   157 ms   163 ms   155 ms  xe-4-0-7.r27.tokyjp05.jp.bb.gin
.ntt.net [129.250.66.89]
  9   158 ms   158 ms   163 ms  ae-1.r30.tokyjp05.jp.bb.gin.ntt
.net [129.250.2.157]
 10   312 ms   310 ms   314 ms  ae-5.r24.tkokhk01.hk.bb.gin.ntt
.net [129.250.2.97]
 11   209 ms   224 ms   208 ms  ae-1.r03.tkokhk01.hk.bb.gin.ntt
.net [129.250.6.98]
 12   213 ms   234 ms     *     ae-1.a01.newthk03.hk.bb.gin.ntt
.net [129.250.5.253]
 13   216 ms   215 ms   218 ms  203.131.254.138
 14   296 ms   294 ms   286 ms  103.235.45.2
 15     *        *        *     请求超时。
 16   288 ms   300 ms   287 ms  103.235.46.39

跟踪完成。

C:\Users\Administrator>
```

实战7：显示主机进程信息的Tasklist命令

Tasklist命令用来显示运行在本地或远程计算机上的所有进程，带有多个执行参数。Tasklist命令的格式如下：

```
Tasklist [/s system [/u username [/p [password]]]] [/m [module] | /svc | /v] [/fi filter] [/fo format] [/nh]
```

利用Tasklist命令可以查看本机中的进程，还可以查看每个进程提供的服务。使用Tasklist命令的具体操作步骤如下。

Step 01 在“命令提示符”中输入Tasklist命令，按Enter键，即可显示本机的所有进程，在显示结果中可以看到映像名称、PID会话名、会话#和内存使用等5部分，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe

C:\Users\Administrator>Tasklist

映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0         24 K
smss.exe                       396 Services                   0        120 K
csrss.exe                      604 Services                   0      1,500 K
wininit.exe                    684 Services                   0        264 K
services.exe                   752 Services                   0      4,784 K
lsass.exe                      760 Services                   0     11,120 K
svchost.exe                    880 Services                   0        200 K
fontdrvhost.exe                892 Services                   0         24 K
WUDFHost.exe                   908 Services                   0        924 K
svchost.exe                    948 Services                   0     15,028 K
svchost.exe                    540 Services                   0      8,840 K
svchost.exe                    576 Services                   0      3,912 K
svchost.exe                   1204 Services                   0      3,536 K
svchost.exe                   1232 Services                   0      2,704 K
svchost.exe                   1292 Services                   0      3,100 K
svchost.exe                   1376 Services                   0      7,168 K
svchost.exe                   1452 Services                   0      1,652 K
svchost.exe                   1524 Services                   0      1,396 K
svchost.exe                   1600 Services                   0      8,680 K
```

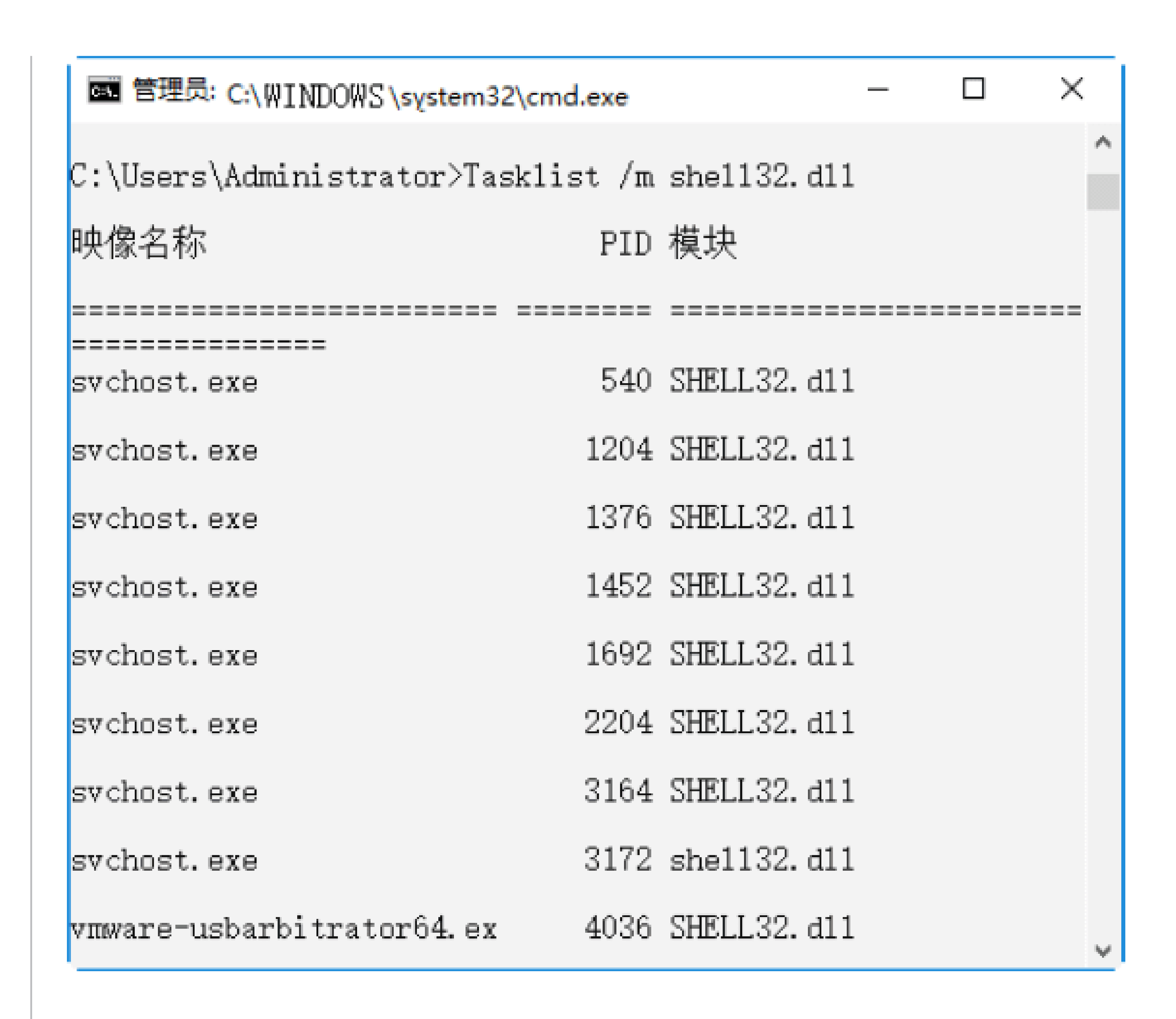
Step 02 使用Tasklist命令可以查看每个进程提供的服务。例如，查看本机进程svchost.exe提供的服务，在“命令提示符”下输入Tasklist /svc命令，按Enter键，即可显示进程svchost.exe提供的服务，如下图所示。

```
管理员: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.16299.15]
(c) 2017 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>Tasklist /svc

映像名称                       PID 服务
========================= ======== ============================================
==
System Idle Process              0 暂缺
System                           4 暂缺
smss.exe                       396 暂缺
csrss.exe                      604 暂缺
wininit.exe                    684 暂缺
services.exe                   752 暂缺
lsass.exe                      760 KeyIso, SamSs, VaultSvc
svchost.exe                    880 PlugPlay
fontdrvhost.exe                892 暂缺
WUDFHost.exe                   908 暂缺
svchost.exe                    948 BrokerInfrastructure, DcomLaunch, Power,
                                   SystemEventsBroker
svchost.exe                    540 RpcEptMapper, RpcSs
svchost.exe                    576 LSM
svchost.exe                   1204 TermService
svchost.exe                   1232 bthserv
svchost.exe                   1292 NcbService
svchost.exe                   1376 Schedule
```

Step 03 如果要查看本地系统中哪些进程调用了shell32.dll模块文件，用户可以在“命令提示符”窗口中输入Tasklist /m shell32.dll命令，按Enter键，即可显示这些进程的列表，如下图所示。



```
管理员: C:\WINDOWS\system32\cmd.exe

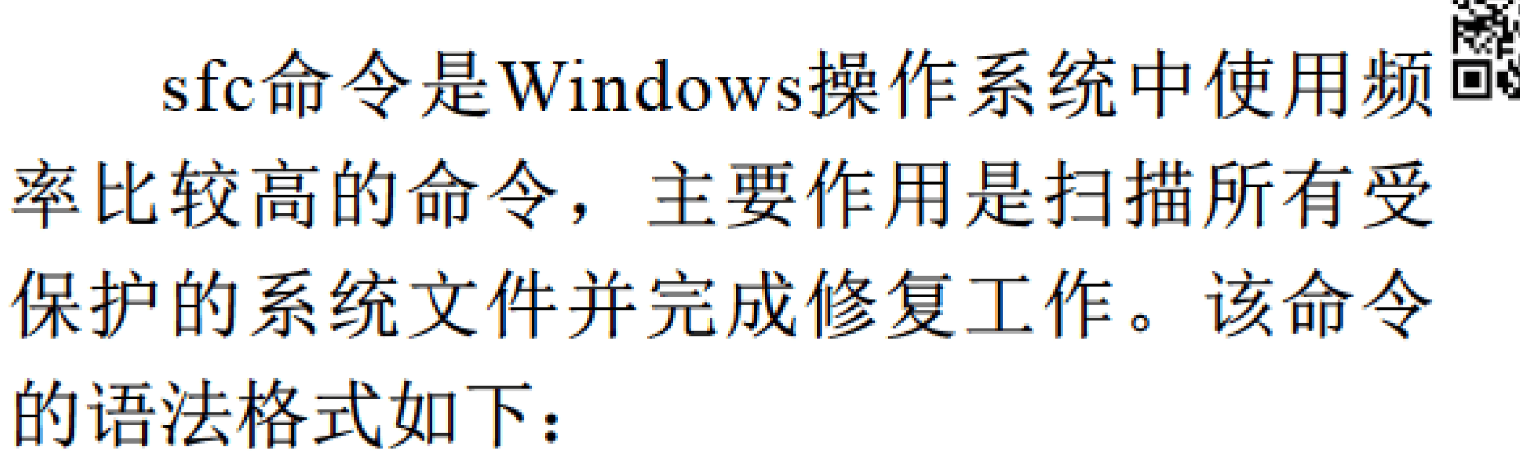
C:\Users\Administrator>Tasklist /m shell32.dll

映像名称                       PID 模块
========================= ======== ============================================
===============
svchost.exe                    540 SHELL32.dll
svchost.exe                   1204 SHELL32.dll
svchost.exe                   1376 SHELL32.dll
svchost.exe                   1452 SHELL32.dll
svchost.exe                   1692 SHELL32.dll
svchost.exe                   2204 SHELL32.dll
svchost.exe                   3164 SHELL32.dll
svchost.exe                   3172 shell32.dll
vmware-usbarbitrator64.ex     4036 SHELL32.dll
```

实战8：扫描并修复系统错误的sfc命令



sfc命令是Windows操作系统中使用频率比较高的命令，主要作用是扫描所有受保护的系统文件并完成修复工作。该命令的语法格式如下：



```
sfc"/scannow""/scanonce""/scanboot""/revert""/purgecache""/cachesize=x"
```

其中，各个参数的含义如下。

（1）/scannow：立即扫描所有受保护的系统文件。

（2）/scanonce：下次启动时，扫描所有受保护的系统文件。

（3）/scanboot：每次启动时，扫描所有受保护的系统文件。

（4）/revert：将扫描返回到默认设置。

（5）/purgecache：清除文件缓存。

（6）/cachesize=x：设置文件缓存大小。

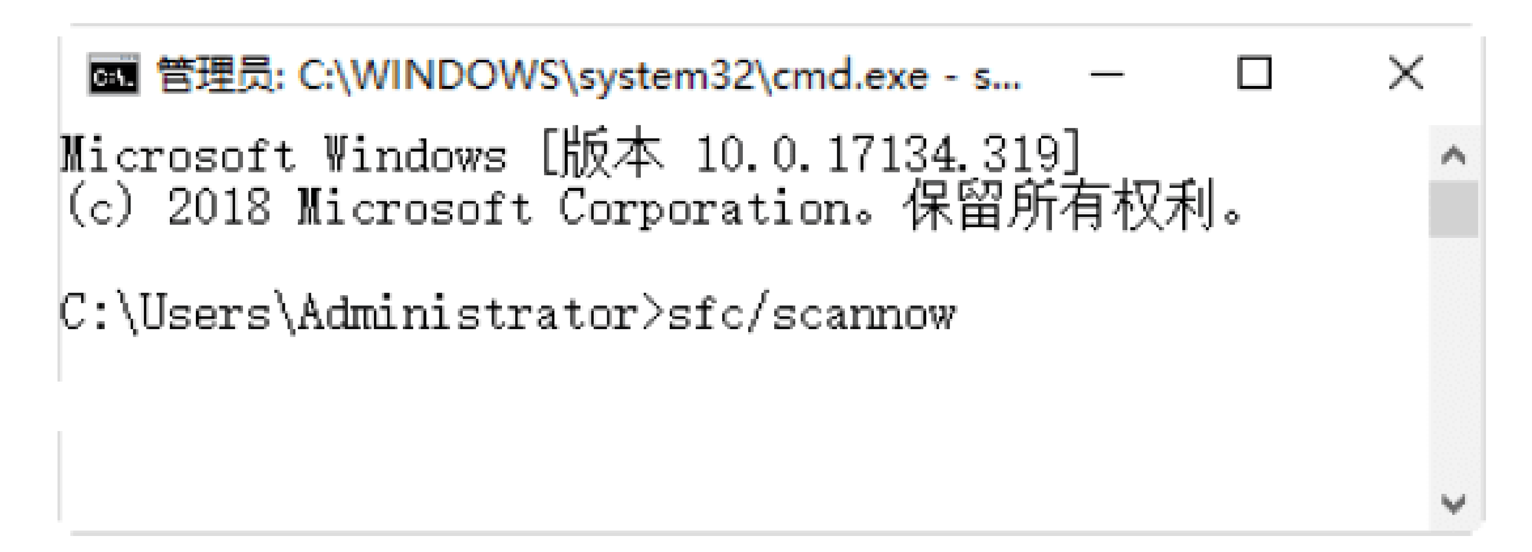
下面以最常用的sfc/scannow为例进行讲解，具体操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“命令提示符（管理员）”选项，如下图所示。

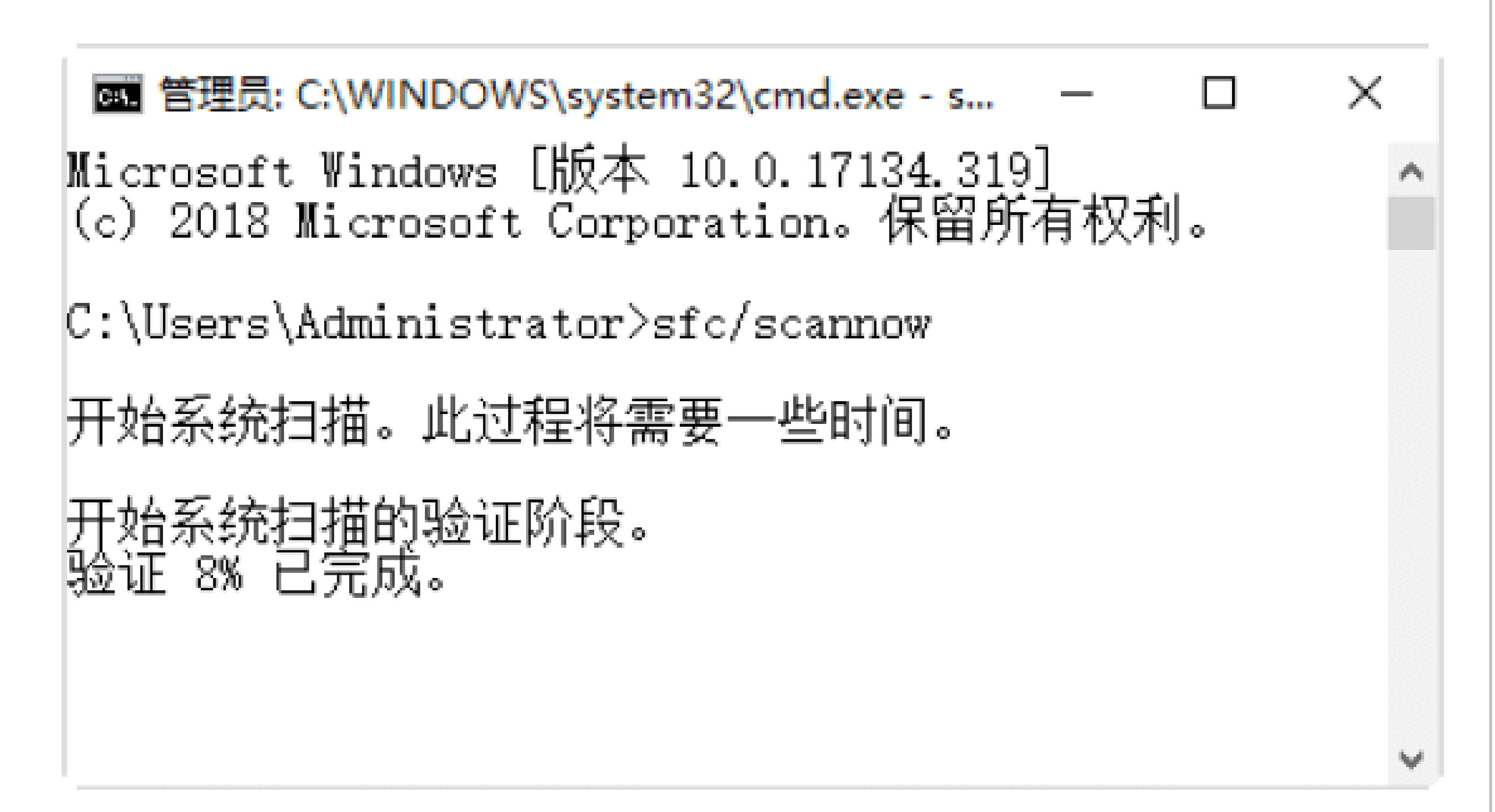




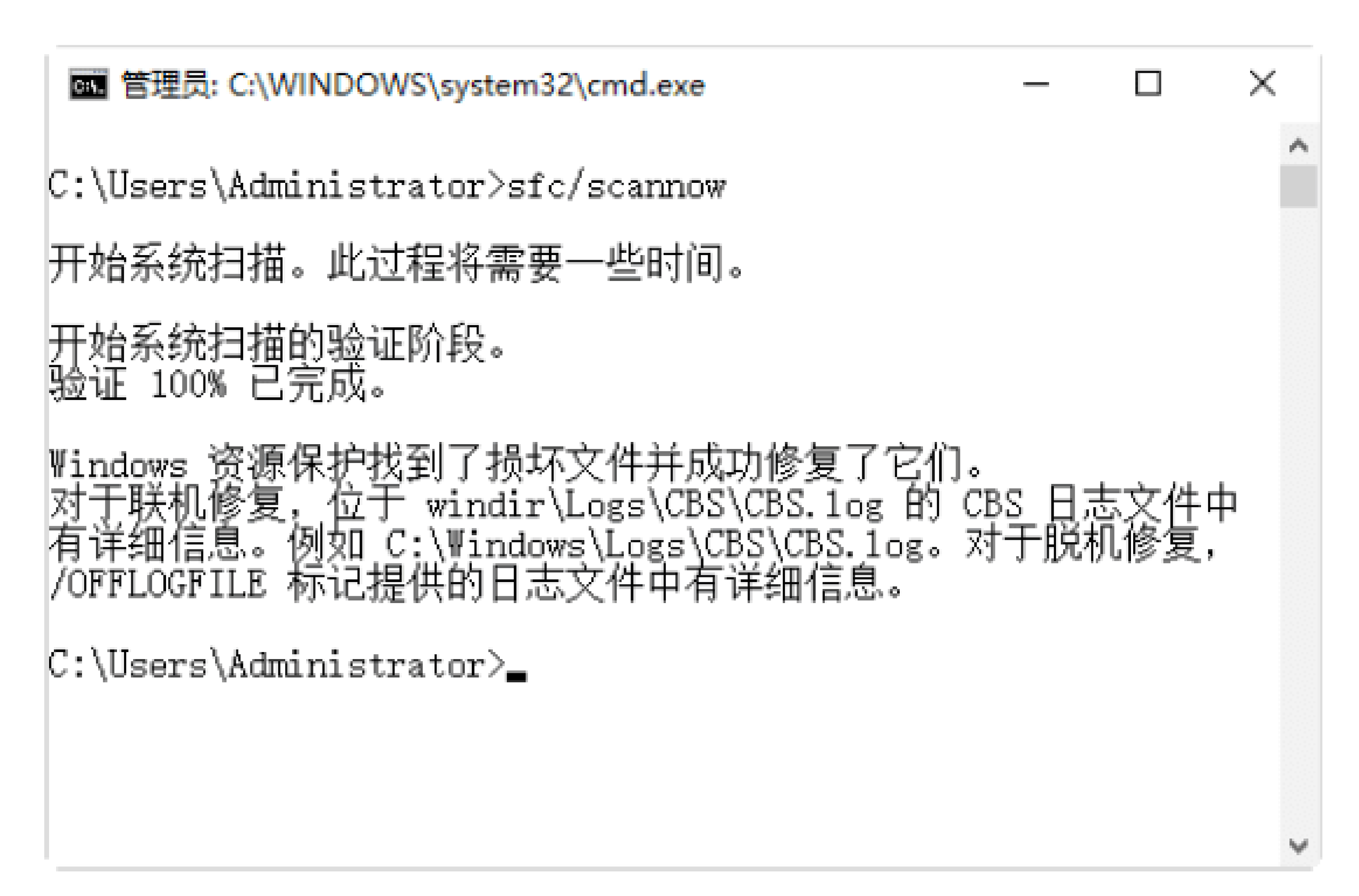
Step 02 弹出“管理员：命令提示符”窗口，输入sfc/scannow命令，按Enter键确认，如下图所示。



Step 03 开始自动扫描系统，并显示扫描的进度，如下图所示。



Step 04 在扫描的过程中，如果发现损坏的系统文件，会自动进行修复操作，并显示修复后的信息，如下图所示。



3.3　实战演练

实战演练1——使用命令代码清除系统垃圾文件

使用批处理文件可以快速地清除计算机中的垃圾文件。下面将介绍使用批处理文件清除系统垃圾文件的具体步骤。

Step 01 打开记事本文件，在其中输入可以清除系统垃圾的代码，如下图所示。

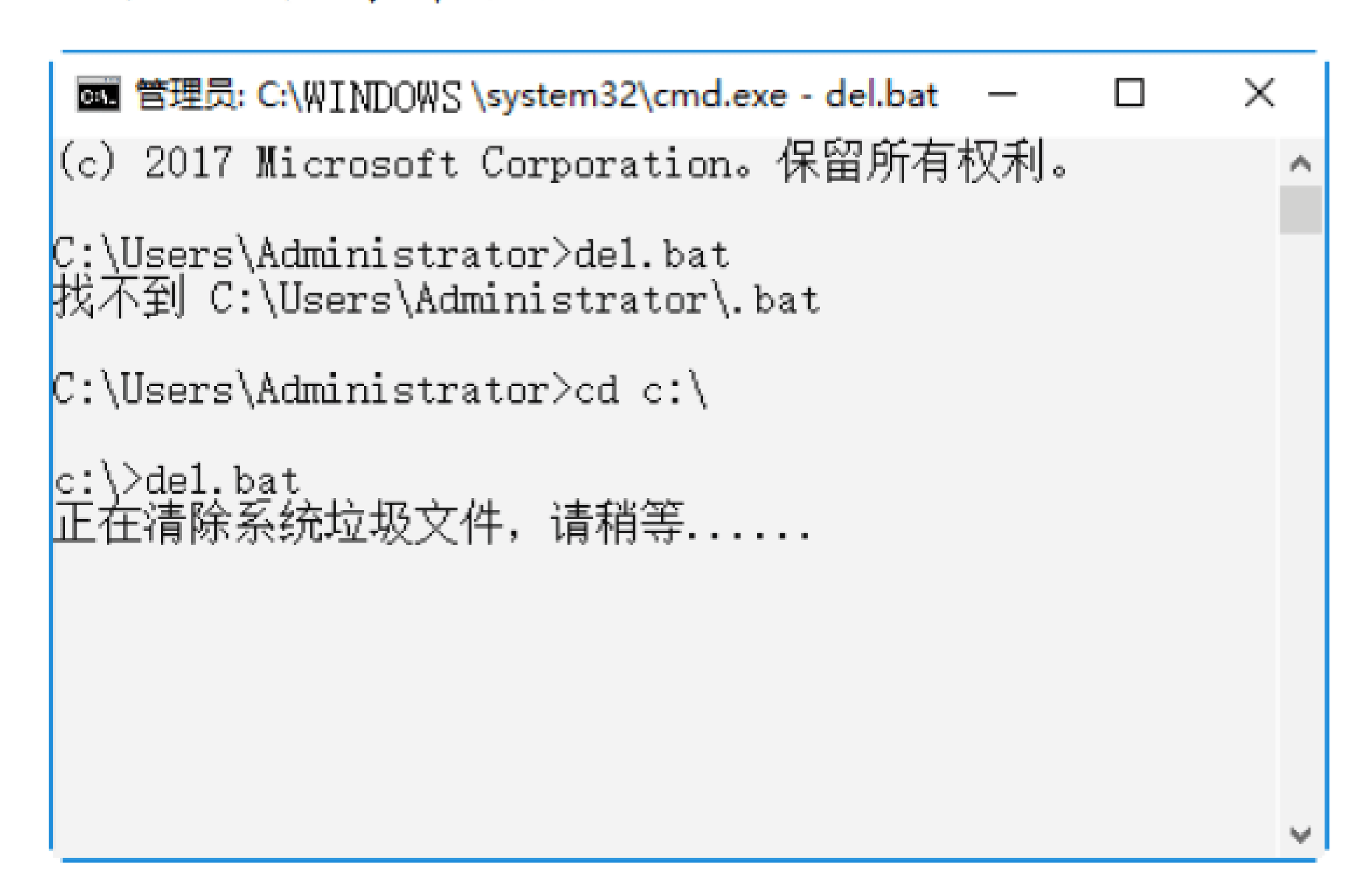
del - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
@echo off
echo 正在清除系统垃圾文件，请稍等......
del /f /s /q %systemdrive%*.tmp
del /f /s /q %systemdrive%*._mp
del /f /s /q %systemdrive%*.log
del /f /s /q %systemdrive%*.gid
del /f /s /q %systemdrive%*.chk
del /f /s /q %systemdrive%*.old
del /f /s /q %systemdrive%\recycled*.*
del /f /s /q %windir%*.bak
del /f /s /q %windir%\prefetch*.*
rd /s /q %windir%\temp & md %windir%\temp
del /f /q %userprofile%\cookies*.*
del /f /q %userprofile%\recent*.*
del /f /s /q "%userprofile%\Local Settings\Temporary Internet Files*.*"
del /f /s /q "%userprofile%\Local Settings\Temp*.*"
del /f /s /q "%userprofile%\recent*.*"
echo 清除系统垃圾完成!
echo. & pause

```
@echo off
echo 正在清除系统垃圾文件，请稍等......
del /f /s /q %systemdrive%\*.tmp
del /f /s /q %systemdrive%\*._mp
del /f /s /q %systemdrive%\*.log
del /f /s /q %systemdrive%\*.gid
del /f /s /q %systemdrive%\*.chk
del /f /s /q %systemdrive%\*.old
del /f /s /q %systemdrive%\recycled\*.*
del /f /s /q %windir%\*.bak
del /f /s /q %windir%\prefetch\*.*
rd /s /q %windir%\temp & md %windir%\temp
del /f /q %userprofile%\cookies\*.*
del /f /q %userprofile%\recent\*.*
del /f /s /q "%userprofile%\Local Settings\Temporary Internet Files\*.*"
del /f /s /q "%userprofile%\Local Settings\Temp\*.*"
del /f /s /q "%userprofile%\recent\*.*"
echo 清除系统垃圾完成!
echo. & pause
```

将上面的代码保存为del.bat。

Step 02 在“命令提示符”窗口中输入del.bat命令，按Enter键，就可以快速清理系统垃

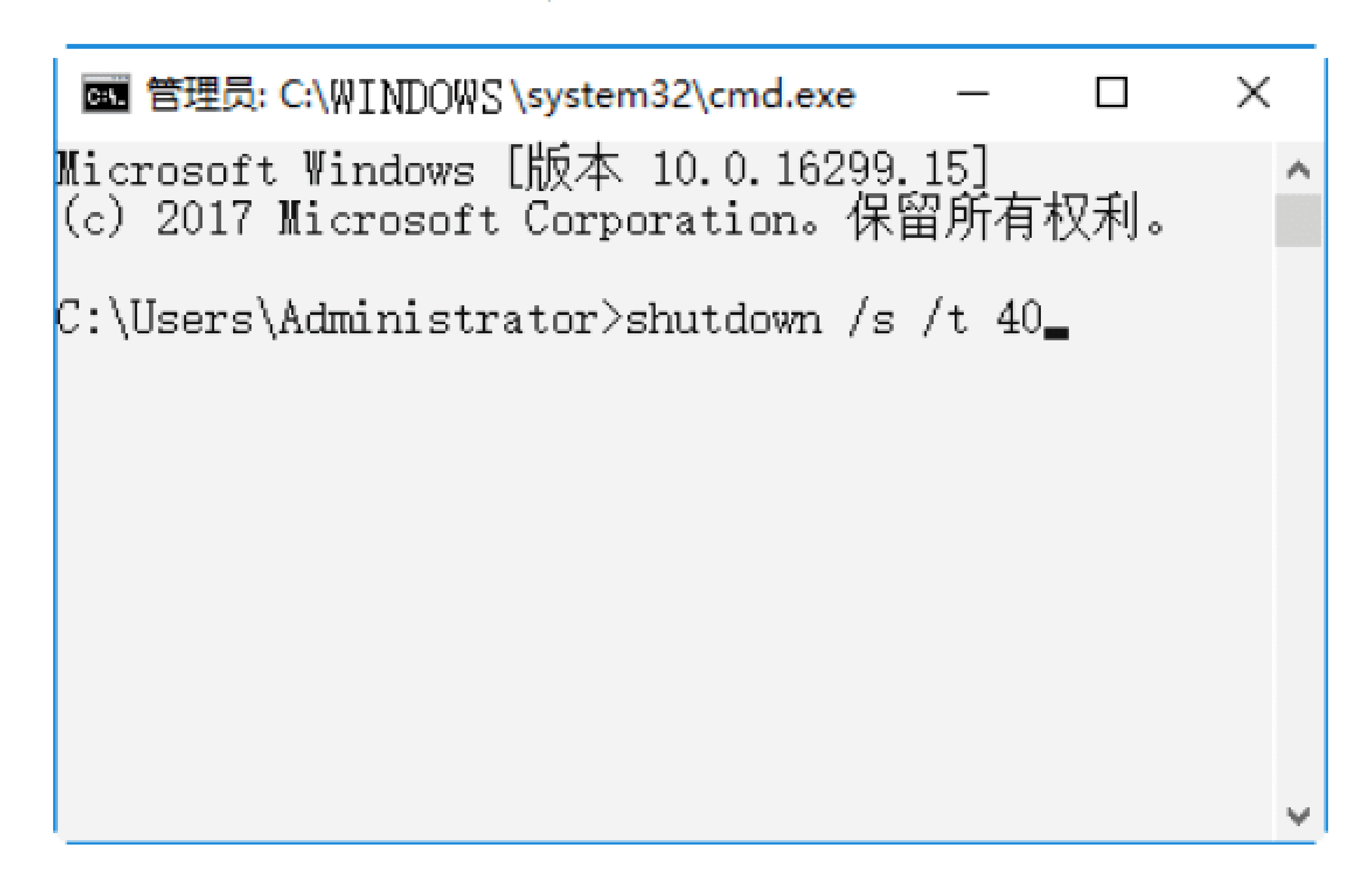
圾，如下图所示。



实战演练2——使用shutdown命令实现定时关机

使用shutdown命令可以实现定时关机的功能，具体操作步骤如下。

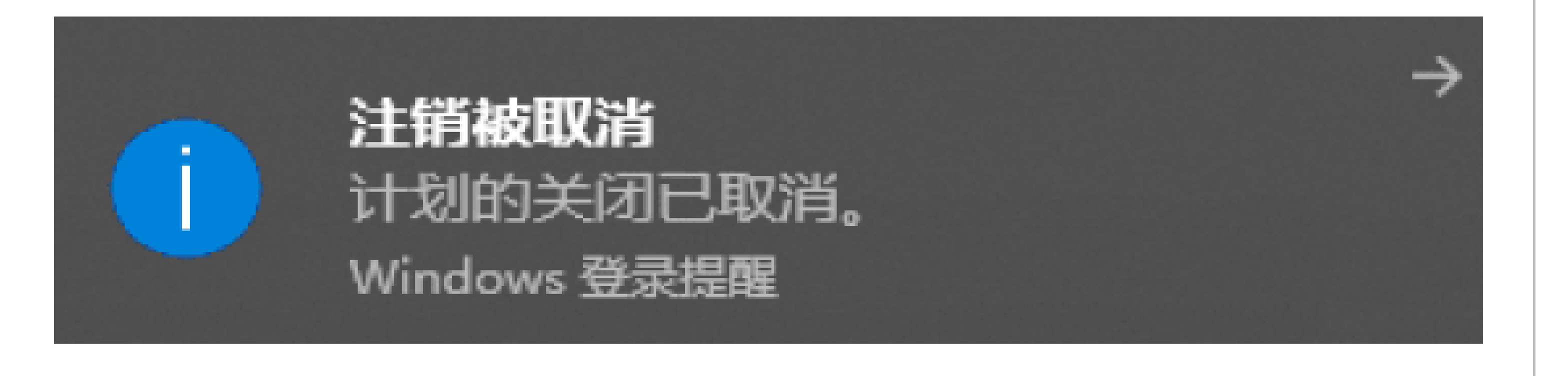
Step 01 在“命令提示符”窗口中输入shutdown /s /t 40命令，如下图所示。



Step 02 弹出一个即将注销用户登录的信息提示框，这样计算机就会在规定的时间内关机，如下图所示。



Step 03 如果此时想取消关机操作，可在命令行中输入shutdown /a命令，按Enter键，桌面右下角出现如下图所示的提示框，表示取消成功。



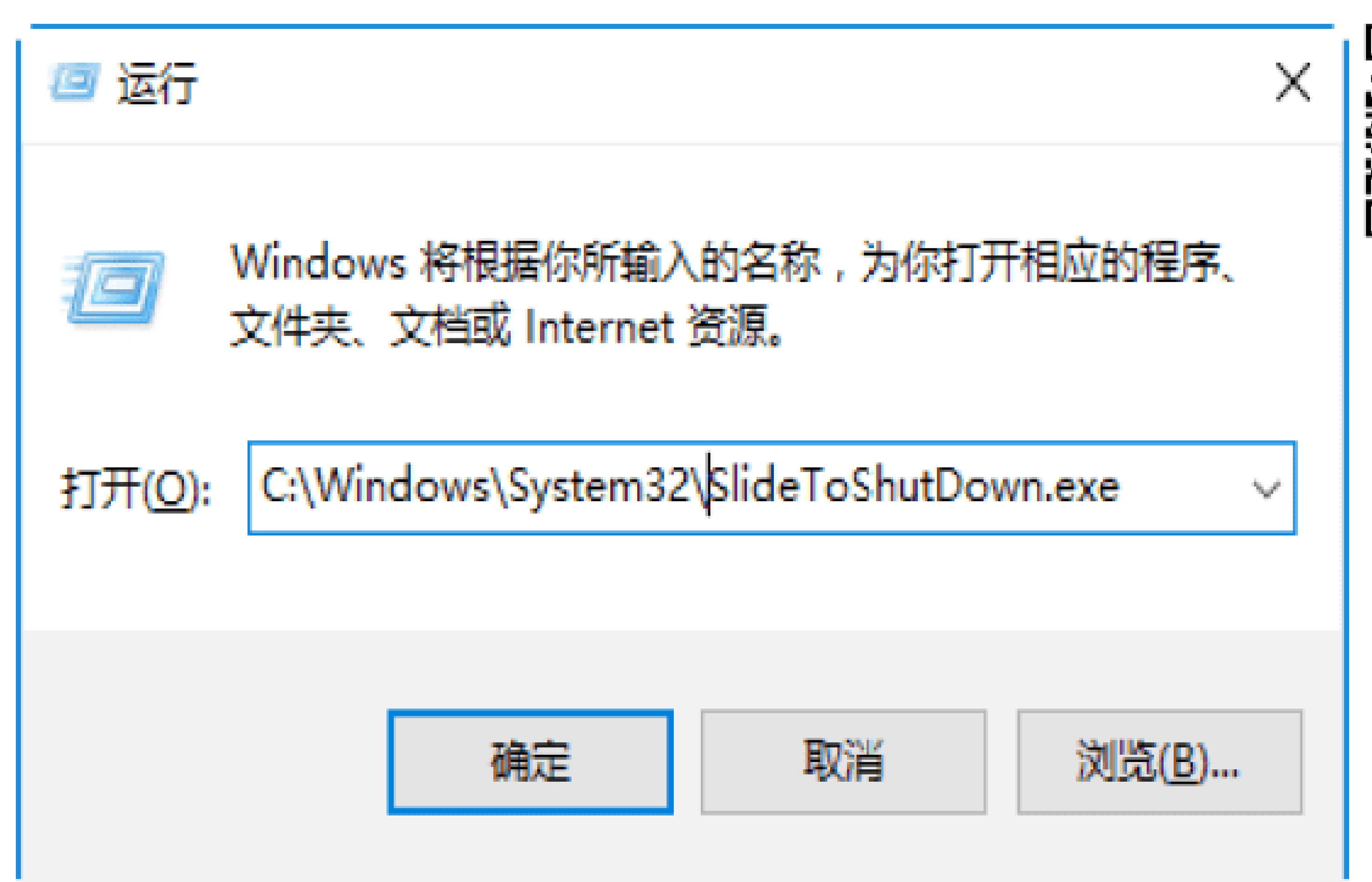
3.4　小试身手

练习1：通过滑动鼠标关闭计算机



在Windows 10操作系统中，用户可以通过鼠标滑动来关机，具体的操作方法如下。

Step 01 按WIN+R组合键，打开“运行”对话框，在文本框中输入C:\Windows\System32\SlideToShutDown.exe命令，单击“确定”按钮，如下图所示。





Step 02 显示如下图所示界面，使用鼠标向下滑动则可关闭计算机，向上滑动则取消操作。如果所用计算机支持触屏操作，也可以手指向下滑动进行关机操作。



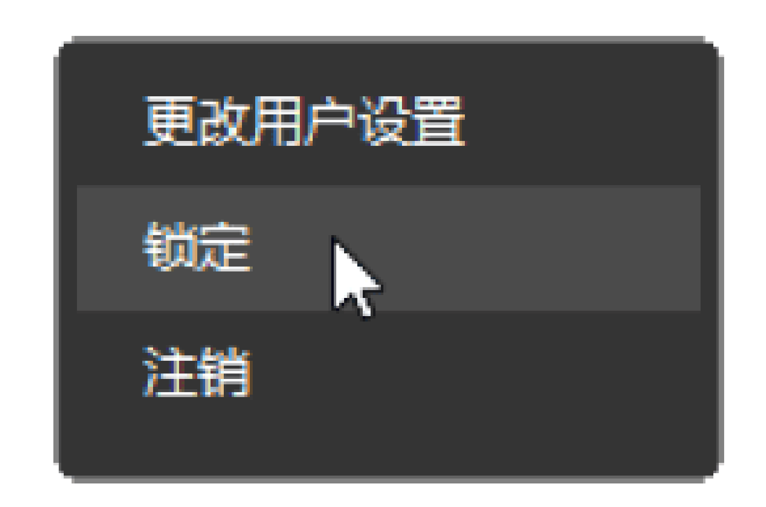
注意：在输入的命令中，执行C盘Windows\system32文件夹下SlideToShutDown.exe应用，如果Windows 10不做C盘，则将C修改为对应的盘符即可，如D、E等。另外，也可以进入对应路径下，找到SlideToShutDown.exe应用，将其发送到桌面，方便使用。



练习2：快速锁定Windows桌面

在离开计算机时，可以将计算机锁屏，这样可以有效地保护桌面隐私。主要有以下两种快速锁屏的方法。

（1）使用菜单命令：按Windows键，弹出开始菜单，单击账户头像，在弹出的快捷菜单中选择“锁定”选项，即可进入锁屏界面，如下图所示。



（2）使用快捷键：按WIN+L组合键，可以快速锁定Windows系统，进入锁屏界面，如下图所示。



第4章　木马病毒的查杀与预防

在网络中，病毒与木马入侵是黑客最常用的入侵方法，从而影响网络和计算机的正常运行。病毒与木马对计算机有着强大的控制和破坏能力，能够盗取目标主机的登录账户和密码、控制目标主机的操作系统和文件等。本章介绍木马病毒的查杀与预防，主要内容包括认识病毒与木马、病毒与木马的查杀与清理等。

4.1　认识病毒与木马

在计算机领域中，病毒与木马是一类恶意程序，具有隐藏性和自发性等特性，可被用来进行恶意行为的攻击。其中，木马又被称为特洛伊木马，是一种基于远程控制的黑客工具，在黑客进行的各种攻击行为中，木马都起到了开路先锋的作用。

4.1.1　常见的木马类型

随着网络技术的发展，现在的木马可谓形形色色，种类繁多，并且还在不断增加，因此，要想一次性列举出所有的木马种类，是不可能的。但是，从木马的主要攻击能力来划分，常见的木马主要有以下几种类型。

1. 网络游戏木马

由于网络游戏中的金钱、装备等虚拟财富与现实财富之间的界限越来越模糊，因此，以盗取网络游戏账号、密码为目的的木马也随之发展泛滥起来。网络游戏木马通常采用记录用户键盘输入、游戏进程、API函数等方法获取用户的密码和账号，窃取到的信息一般通过发送电子邮件或向远程脚本程序提交的方式发送给木马制作者。

2. 网银木马

网银木马是针对网上交易系统编写的木马，其目的是盗取用户的卡号、密码等信息。此类木马的危险非常直接，受害用户的损失也更加惨重。例如“网银大盗”木马，在用户进入银行网银登录页面时，会自动把页面换成安全性能较差、但依然能够运转的老版页面，然后记录用户在此页面上填写的卡号和密码。随着网上交易的普及，受到外来网银木马威胁的用户也在不断增加。

3. 即时通讯软件木马

现在，即时通讯软件百花齐放，如QQ、微信等，而且网上聊天的用户群也十分庞大，常见的即时通讯类木马一般有发送消息型与盗号型。

（1）发送消息型：通过即时通讯软件自动发送含有恶意网址的消息，目的在于让收到消息的用户单击网址激活木马，用户中木马后又会向更多好友发送木马消息，此类木马常用技术是搜索聊天窗口，进而控制该窗口自动发送文本内容。

（2）盗号型：主要目标在于即时通讯软件的登录账号和密码，工作原理和网络游戏木马类似，木马作者盗得他人账号后，可以偷窥聊天记录等隐私内容。

4.破坏性木马

顾名思义，破坏性木马唯一的功能就是破坏感染木马的计算机文件系统，使用户遭受系统崩溃或者重要数据丢失的巨大损失。

4.1.2 认识网络中的病毒

随着网络的普及，病毒也更加泛滥，病毒是一种特殊的计算机程序，病毒能通过修改计算机内的其他程序，并把自身复制到其他程序中，完成对其他程序的感染和侵害，从而抢占计算机系统资源，干扰计算机系统正常的工作。

常见计算机中毒的途径有以下几种。

（1）单击超链接中毒。这种入侵方法主要是在网页中放置恶意代码，引诱用户单击，一旦用户单击超链接，就会感染病毒，因此，不要随便单击网页中的链接。

（2）网站中存在各种恶意代码，借助IE浏览器的漏洞，强制用户安装一些恶意软件，有些顽固的软件很难卸载。建议用户及时更新系统补丁，对于不了解的插件不要随便安装，以免给病毒流行可乘之机。

（3）通过下载附带病毒的软件中毒，有些破解的软件在安装时会附带安装一个病毒程序，而此时用户并不知道。建议用户下载正版的软件，尽量到软件的官方网站下载。如果在其他的网站下载软件，可以先使用杀毒软件查杀。

（4）通过网络广告中毒。上网时经常可以看到一些自动弹出的广告，包括悬浮广告、异常图片等。特别是一些中奖广告，往往带有病毒链接。



4.1.3 计算机中病毒后的表现

一般情况下，计算机病毒是依附某一系统软件或用户程序进行繁殖和扩散，病毒发作时危机计算机的正常工作，破坏数据与程序，侵占计算机资源等。

计算机在感染病毒后的现象如下。

（1）屏幕显示异常，屏幕显示出不是由正常程序产生的画面或字符串，屏幕显示混乱。

（2）程序装入时间增长，文件运行速度下降。

（3）用户并没有访问的设备出现“忙”信号。

（4）磁盘出现莫名其妙的文件和磁盘坏区，卷标也发生变化。

（5）系统自行引导。

（6）丢失数据或程序，文件字节数发生变化。

（7）内存空间、磁盘空间减少。

（8）异常死机。

（9）磁盘访问时间比平常增长。

（10）系统引导时间增长。

（11）程序或数据神秘丢失。

（12）可执行文件的大小发生变化。

（13）出现莫名其妙的隐蔽文件。

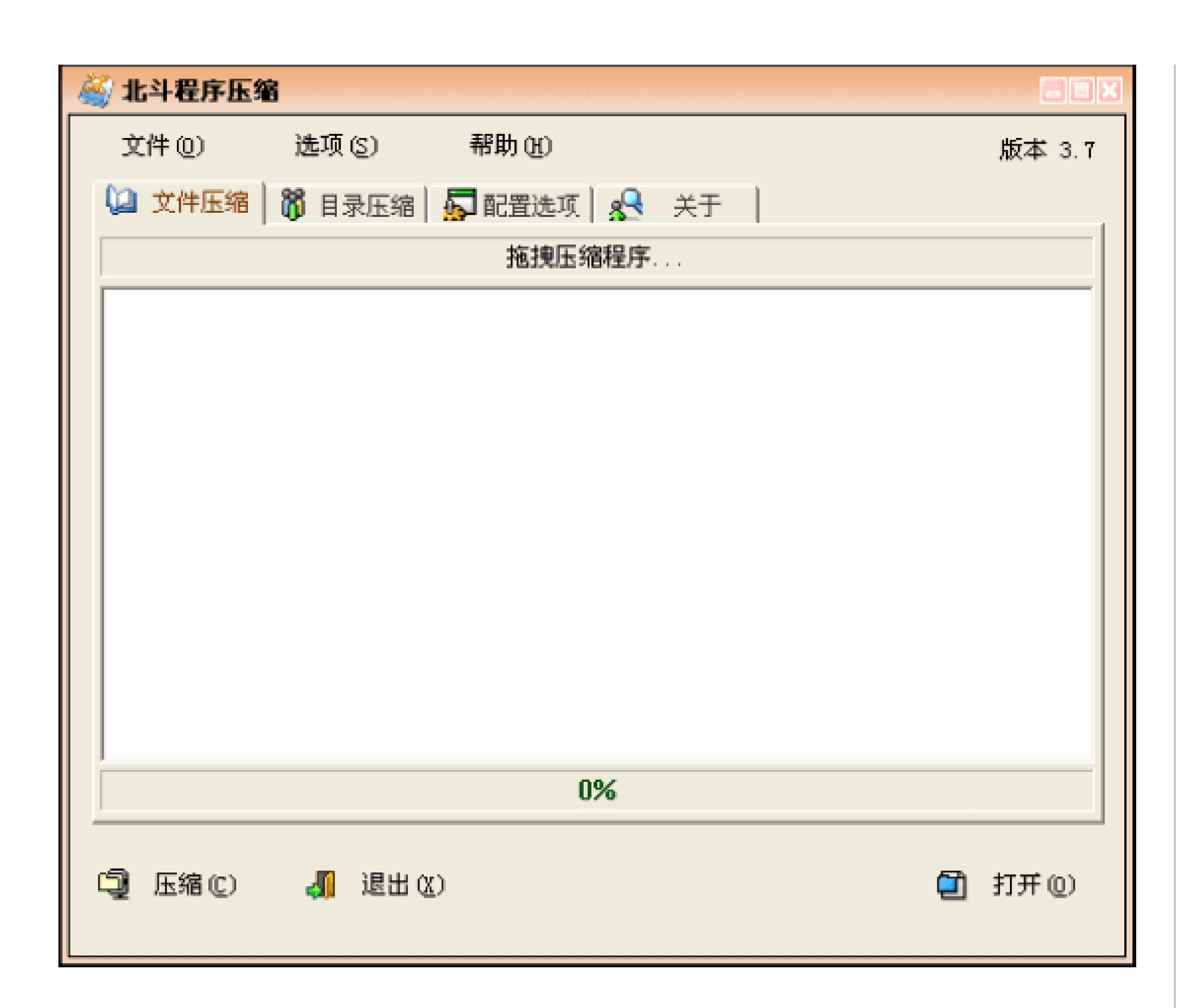
4.2 木马自我保护与伪装手段

在木马清除软件越来越强的情况下，木马不但要具有更强的功能，还要具有自我保护与伪装的手段。目前，大部分杀毒软件是靠特征码来识别木马的，因此，可以通过伪装成其他文件类型或给木马程序加壳来更改木马的特征码，以躲过杀毒软件的查杀。

实战1：通过加壳工具给木马加壳

通过给木马多次加壳，可以将其保护起来，从而保证不会被杀毒软件轻易查杀。“北斗程序压缩（NsPack）”就是一款可以为木马进行多次加壳的工具。具体的操作步骤如下。

Step 01 运行“北斗程序压缩”工具，打开其主窗口，如下图所示。



Step 02 选择“配置选项”选项卡，在其中勾选相应参数前的复选框，如下图所示。



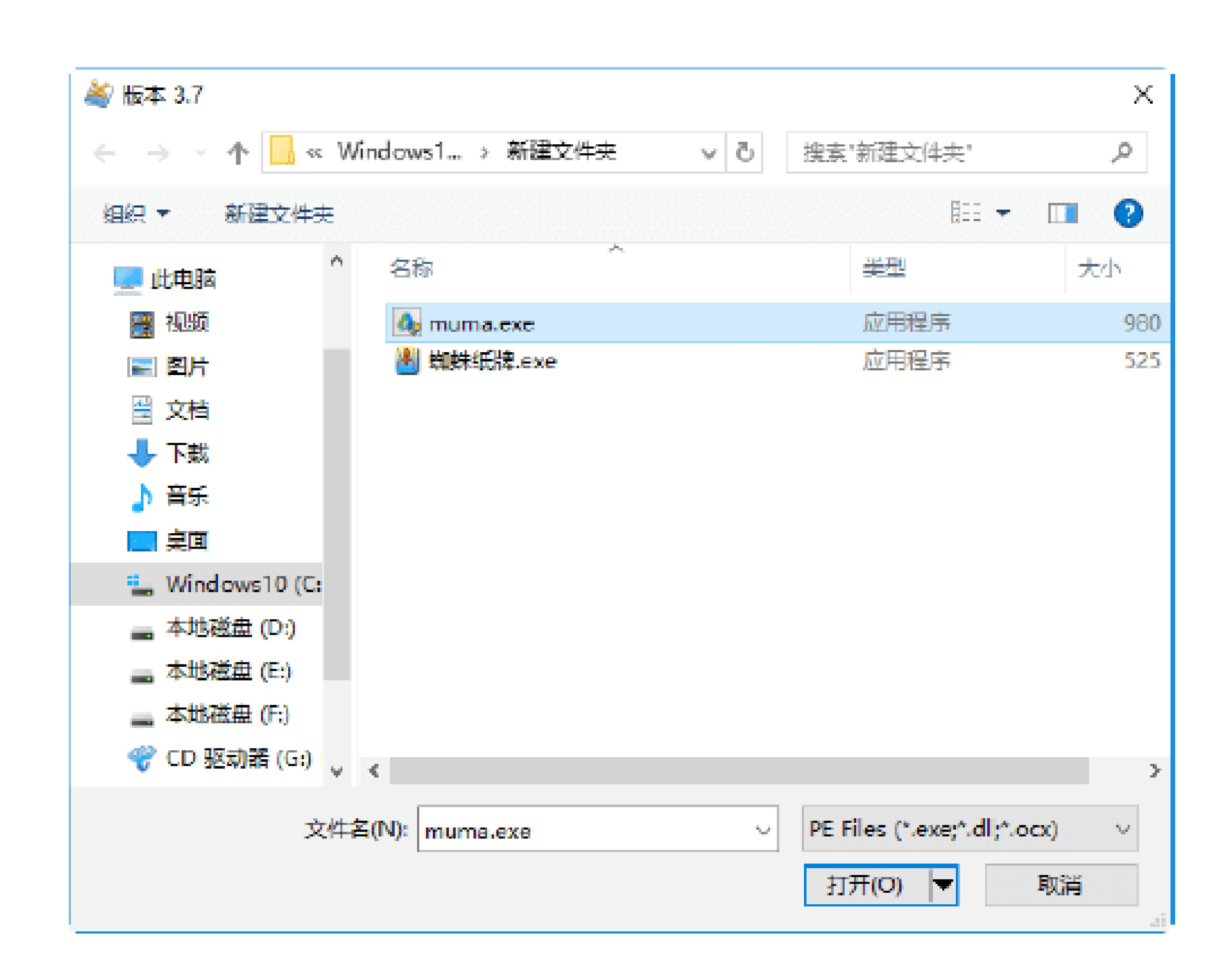
其中有几个比较重要的参数，具体含义如下。

（1）处理共享节：加壳时软件会智能地判断共享节的可用性并做出正确处理，使木马程序在压缩后能够正常使用，此项是必选的。

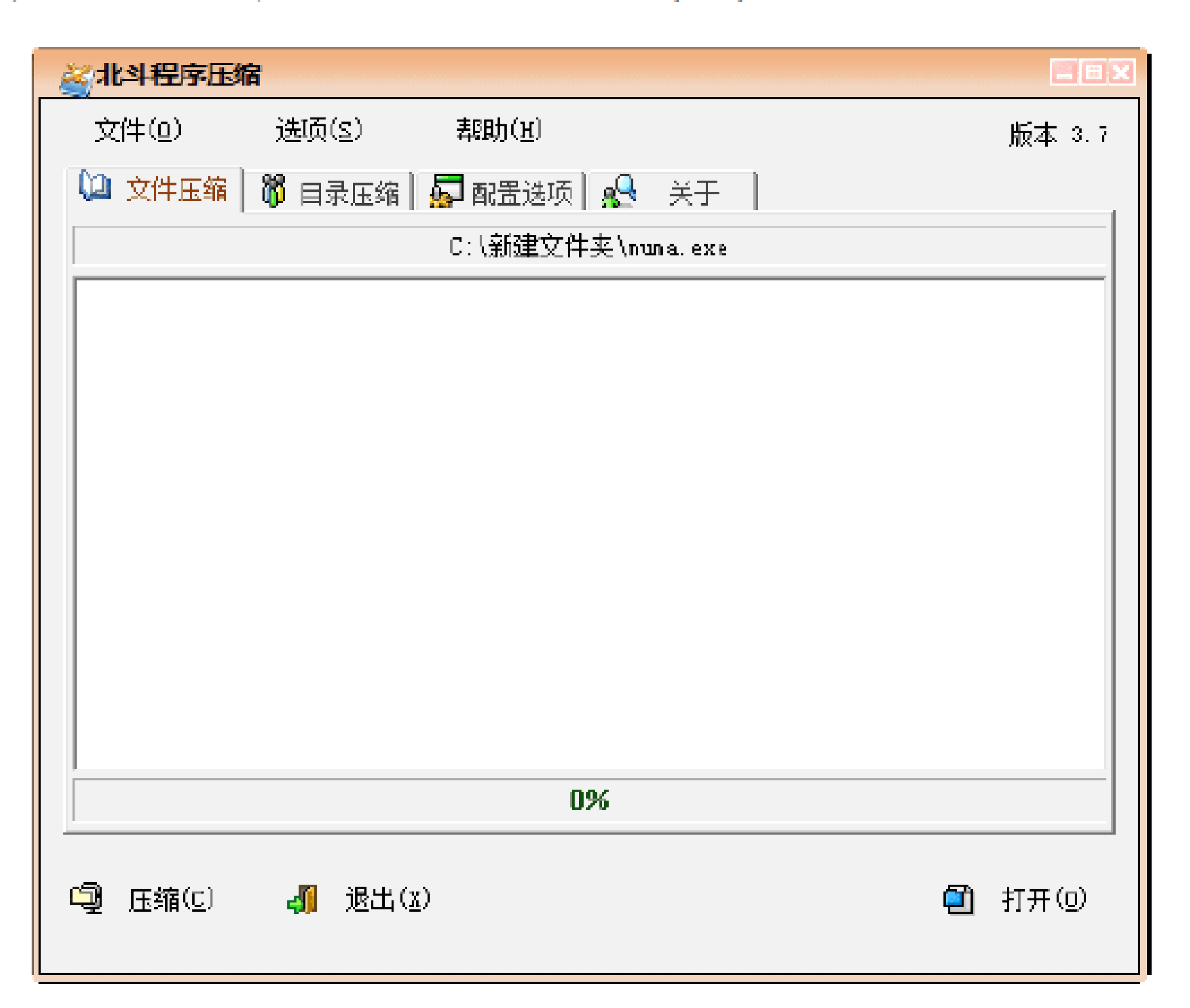
（2）最大程度压缩：压缩加壳生成后的程序体积达到最小。

（3）使用Windows DLL加载器：让Windows自动进行处理。

Step 03 选择“文件压缩”选项卡，单击“打开”按钮，即可打开“版本3.7”对话框，在其中选择一个可执行文件，如下图所示。



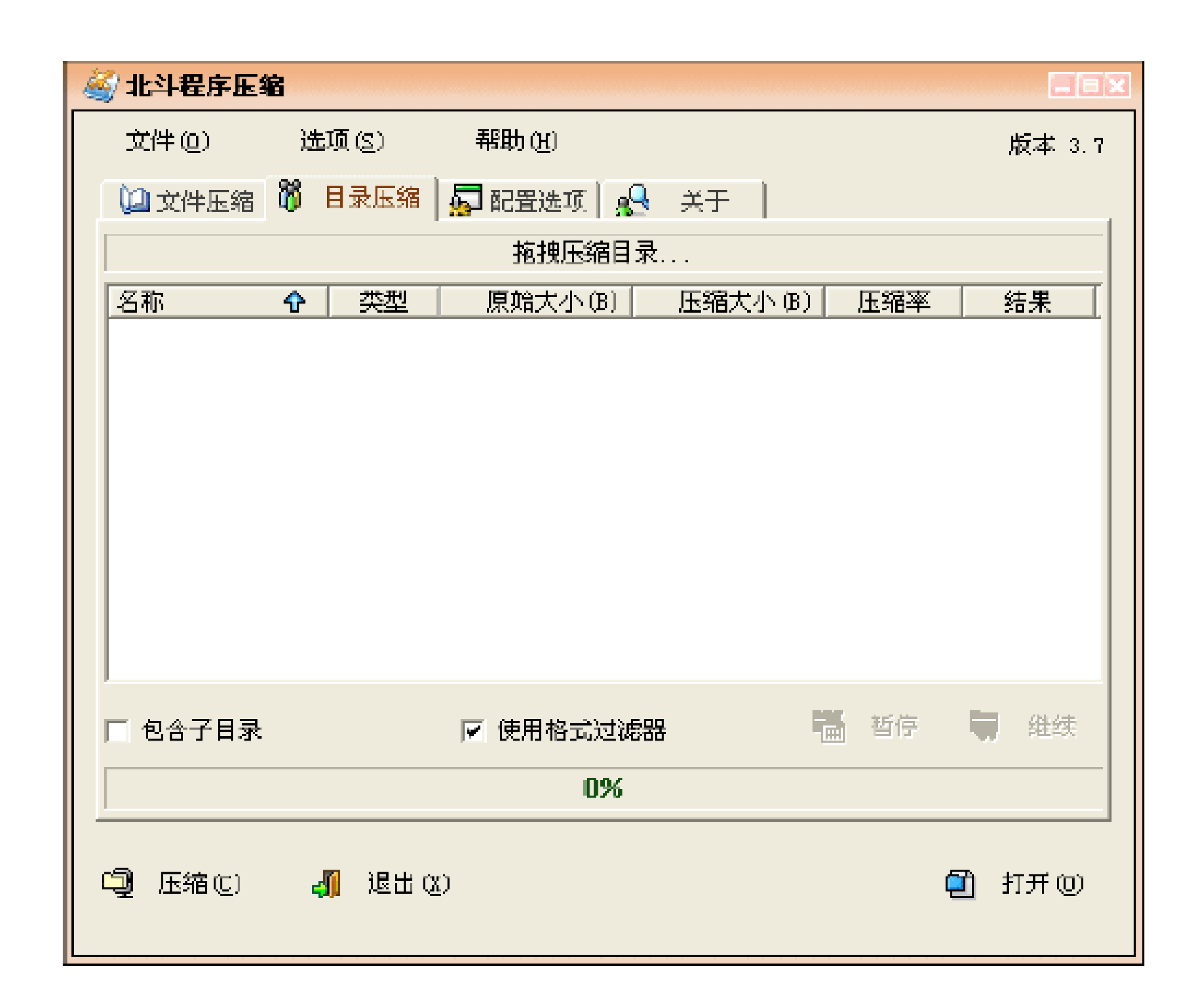
Step 04 单击“打开”按钮，返回到“文件压缩”选项卡，在空白窗格上显示要加壳文件的路径和名称，如下图所示。



Step 05 单击“压缩”按钮，即可开始文件的压缩，如下图所示。

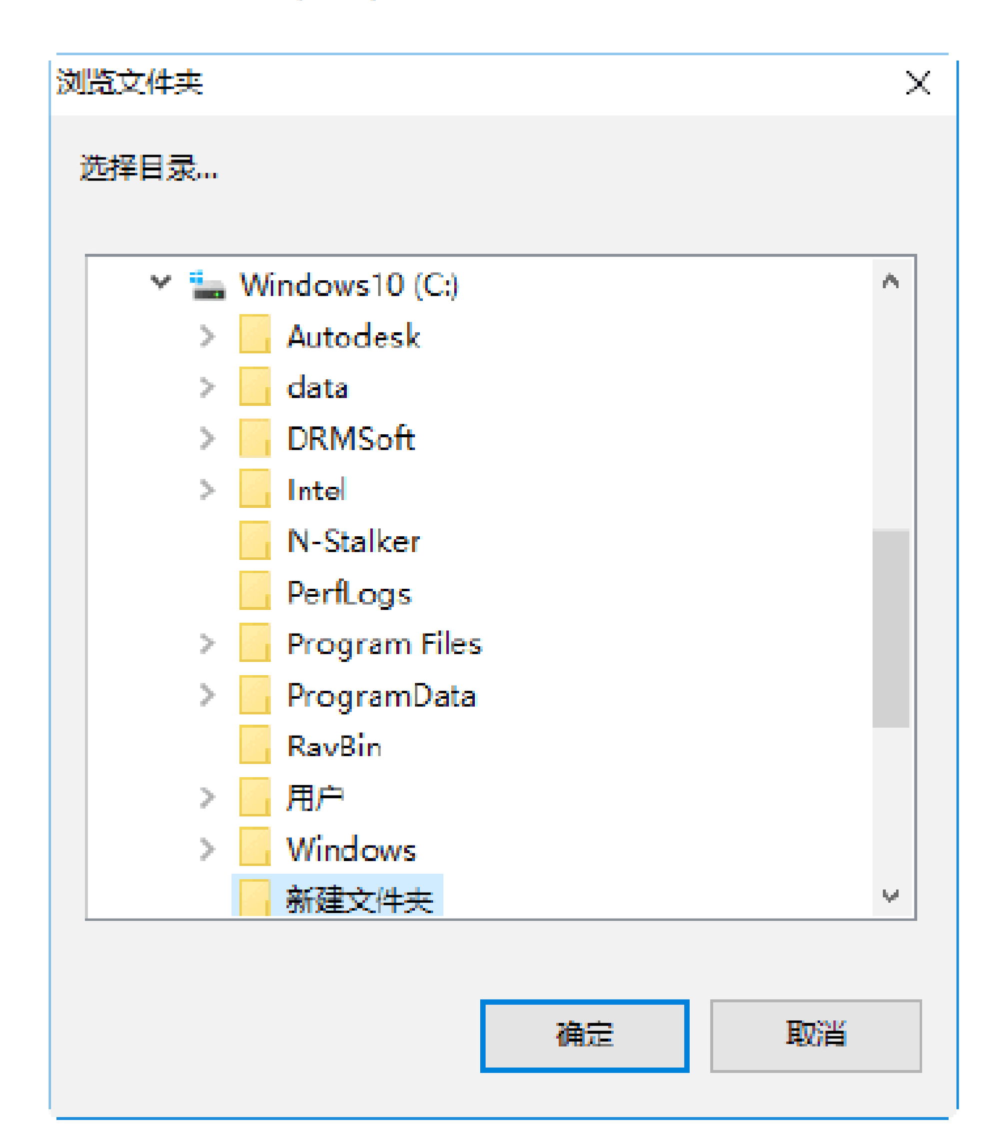


Step 06 当需要一次性对大量的木马程序进行压缩加壳时，可以使用“北斗程序压缩”的“目录压缩”功能，选择“目录压缩”选项卡，进入“目录压缩”设置界面，如下图所示。





Step 07 单击“打开”按钮，即可打开“浏览文件夹”对话框，在其中选择需要压缩的文件夹，如下图所示。



Step 08 单击“确定”按钮，返回到“目录压缩”选项卡，即可看到添加的文件以及其子目录，勾选“包含子目录”复选框和“使用格式过滤器”复选框，如下图所示。



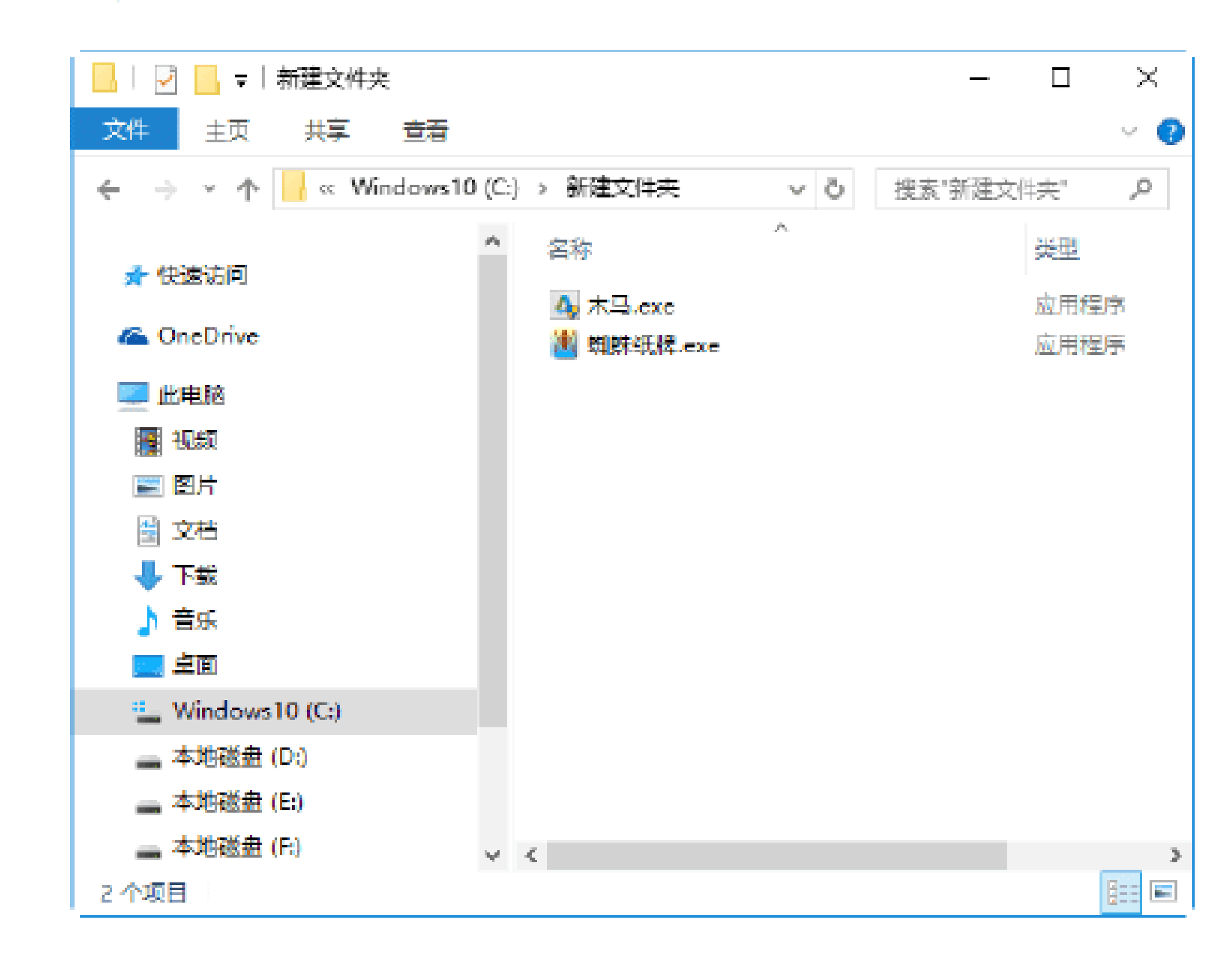
Step 09 单击“压缩”按钮，即可开始对选中的程序进行批量压缩加壳，如下图所示。



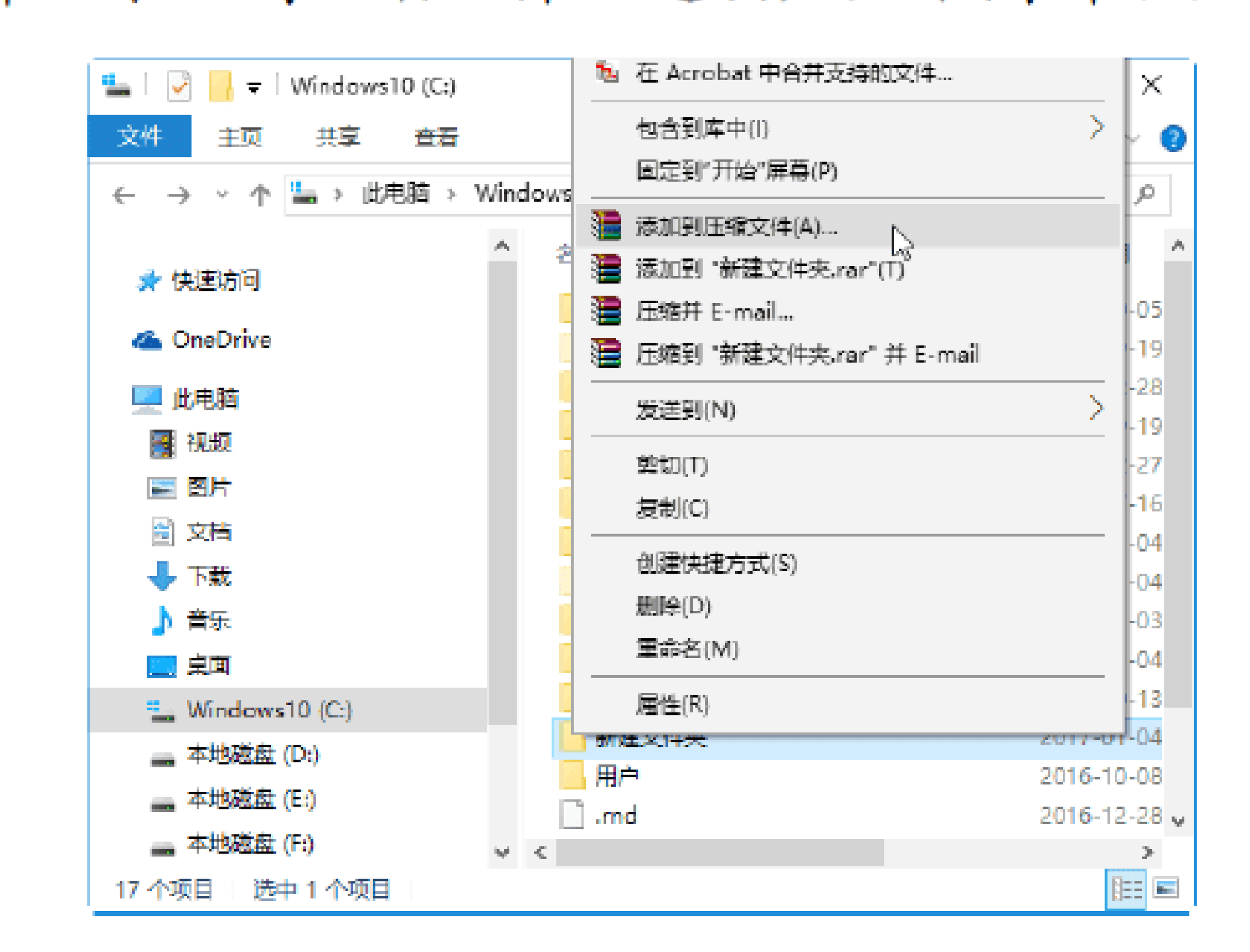
实战2：使用WinRAR伪装木马

利用WinRAR的压缩功能可以将正常的文件与木马捆绑在一起，并生成自解压文件，一旦用户运行该文件，同时也会激活木马文件，这是木马常用的伪装手段之一。具体的操作步骤如下。

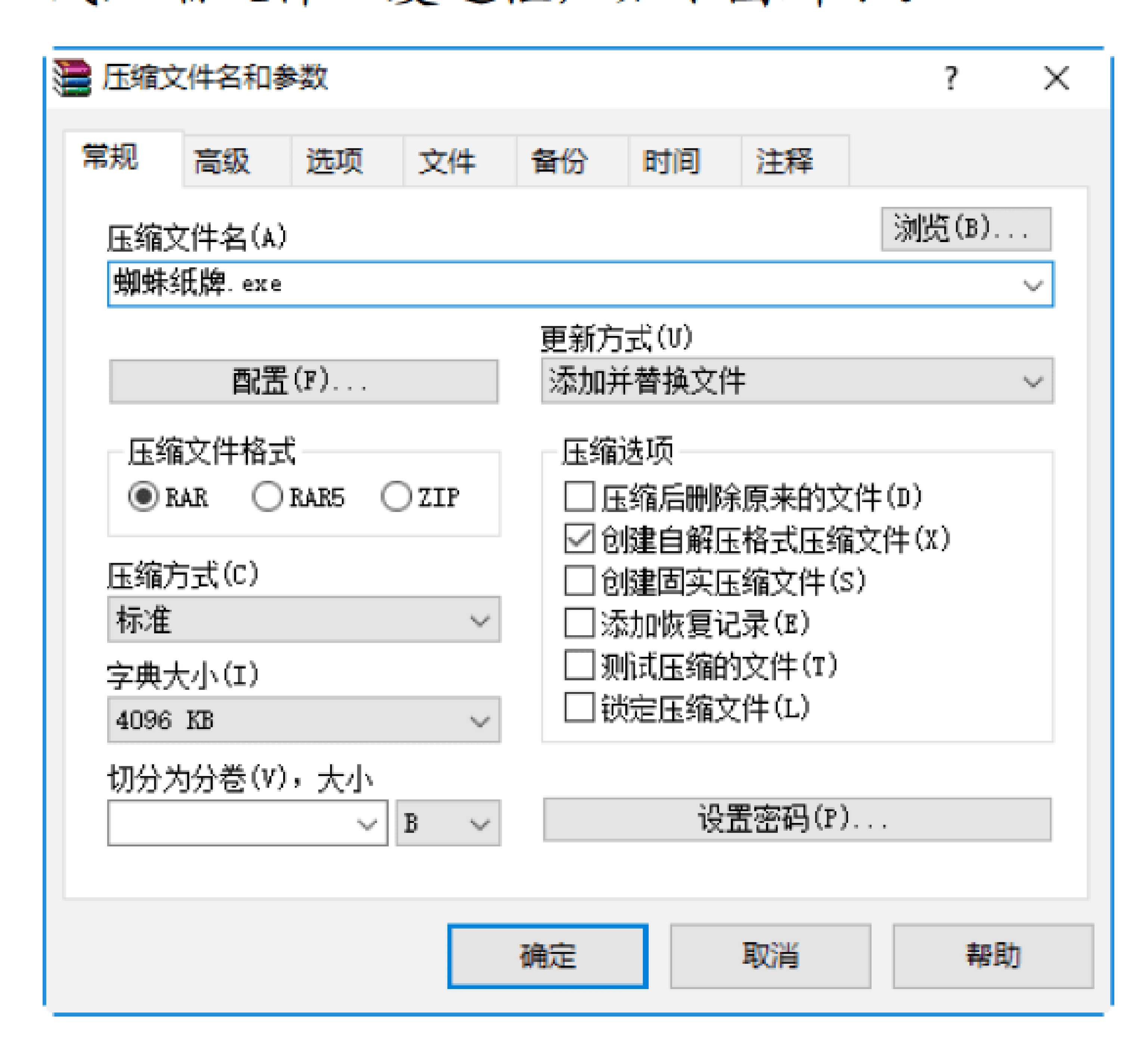
Step 01 准备好要捆绑的文件，这里选择的是一个蜘蛛纸牌和木马文件（木马.exe），并存放在同一个文件夹下，如下图所示。



Step 02 选中蜘蛛纸牌和木马文件（木马.exe）所在的文件夹，右击，在弹出的快捷菜单中选择“添加到压缩文件”选项，如下图所示。



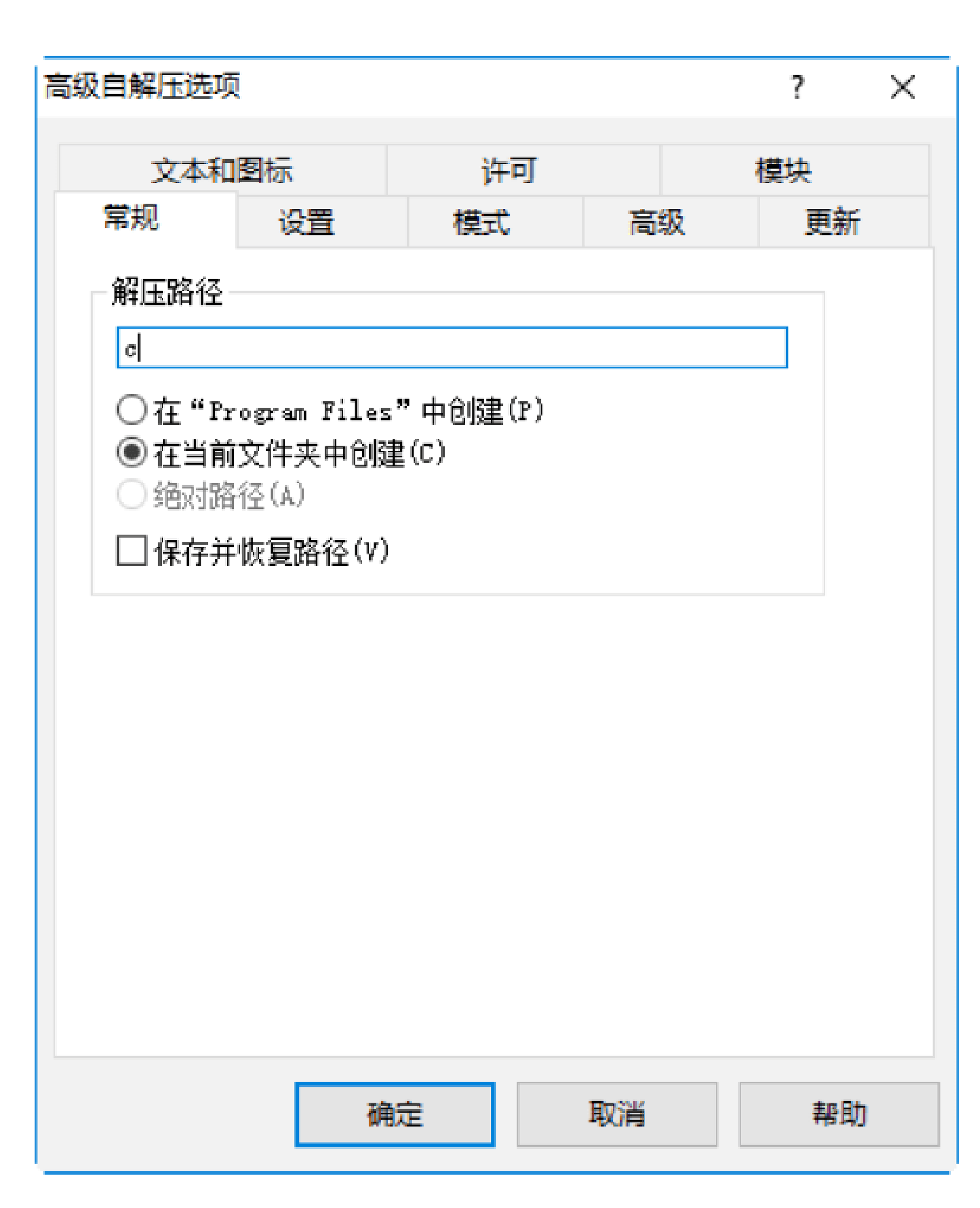
Step 03 打开“压缩文件名和参数”对话框。在“压缩文件名”文本框中输入要生成的压缩文件的名称，并勾选“创建自解压格式压缩文件”复选框，如下图所示。



Step 04 选择“高级”选项卡，在其中勾选“保存文件安全数据”“保存文件流数据”“后台压缩”“完成操作后关闭计算机电源”“如果其他WinRAR副本被激活则等待”复选框，如下图所示。

压缩文件名和参数
常规 高级 选项 文件 备份 时间 注释
NTFS 选项
保存文件安全数据(S)
保存文件流数据(T)
将符号链接保存为链接(L)
将硬链接保存为链接(H)
恢复记录(R)
3 %
分卷
每个分卷操作完之后暂停(V)
旧风格分卷名(L)
0 个恢复卷(C)
压缩(C)...
自解压选项(X)...
系统
后台压缩(B)
完成操作后关闭计算机电源(F)
如果其它 WinRAR 副本被激活则等待(W)
确定 取消 帮助

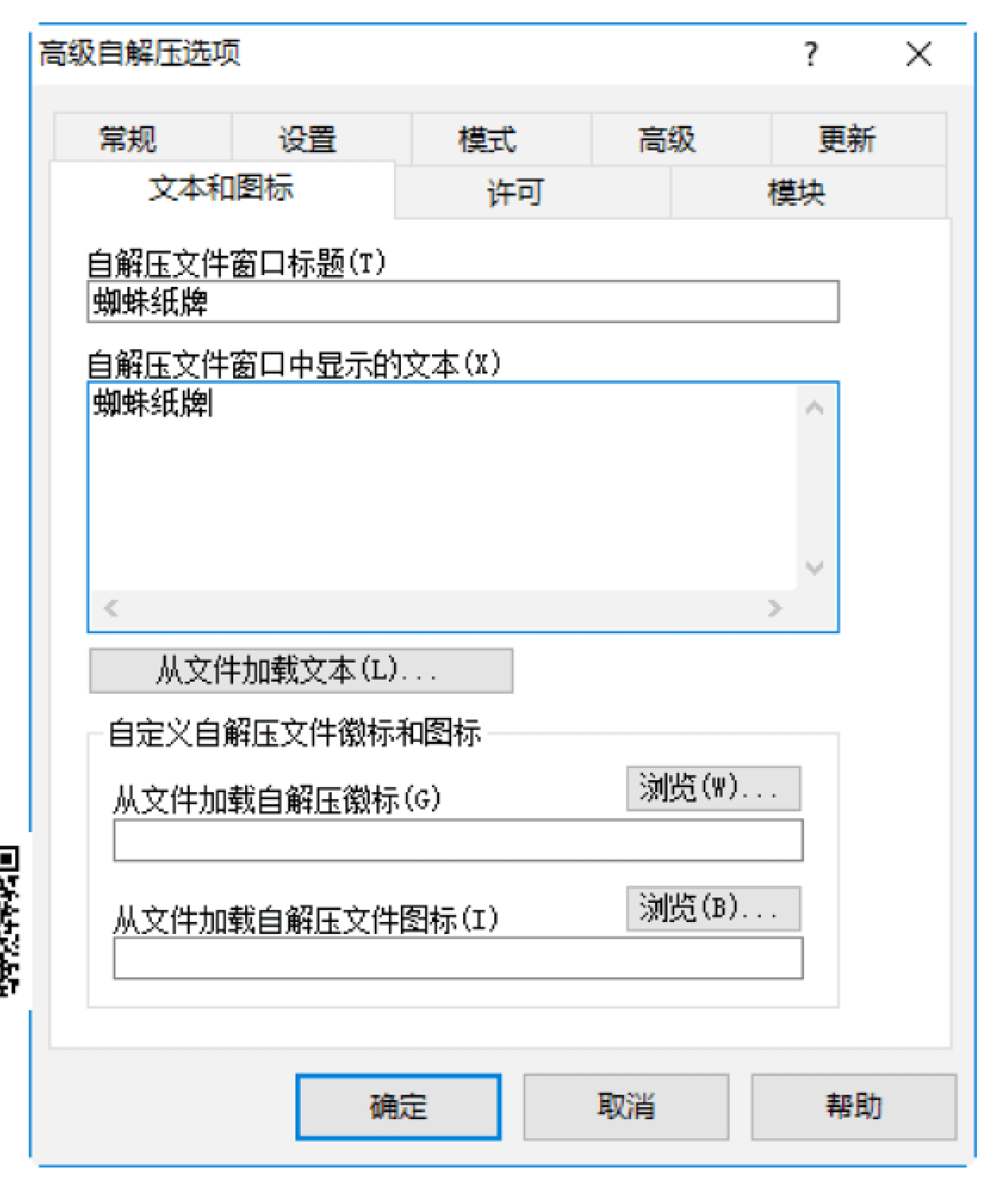
Step 05 单击“自解压选项”按钮，即可打开“高级自解压选项”对话框，在“解压路径”文本框中输入解压路径，并选中“在当前文件夹中创建”单选按钮，如下图所示。



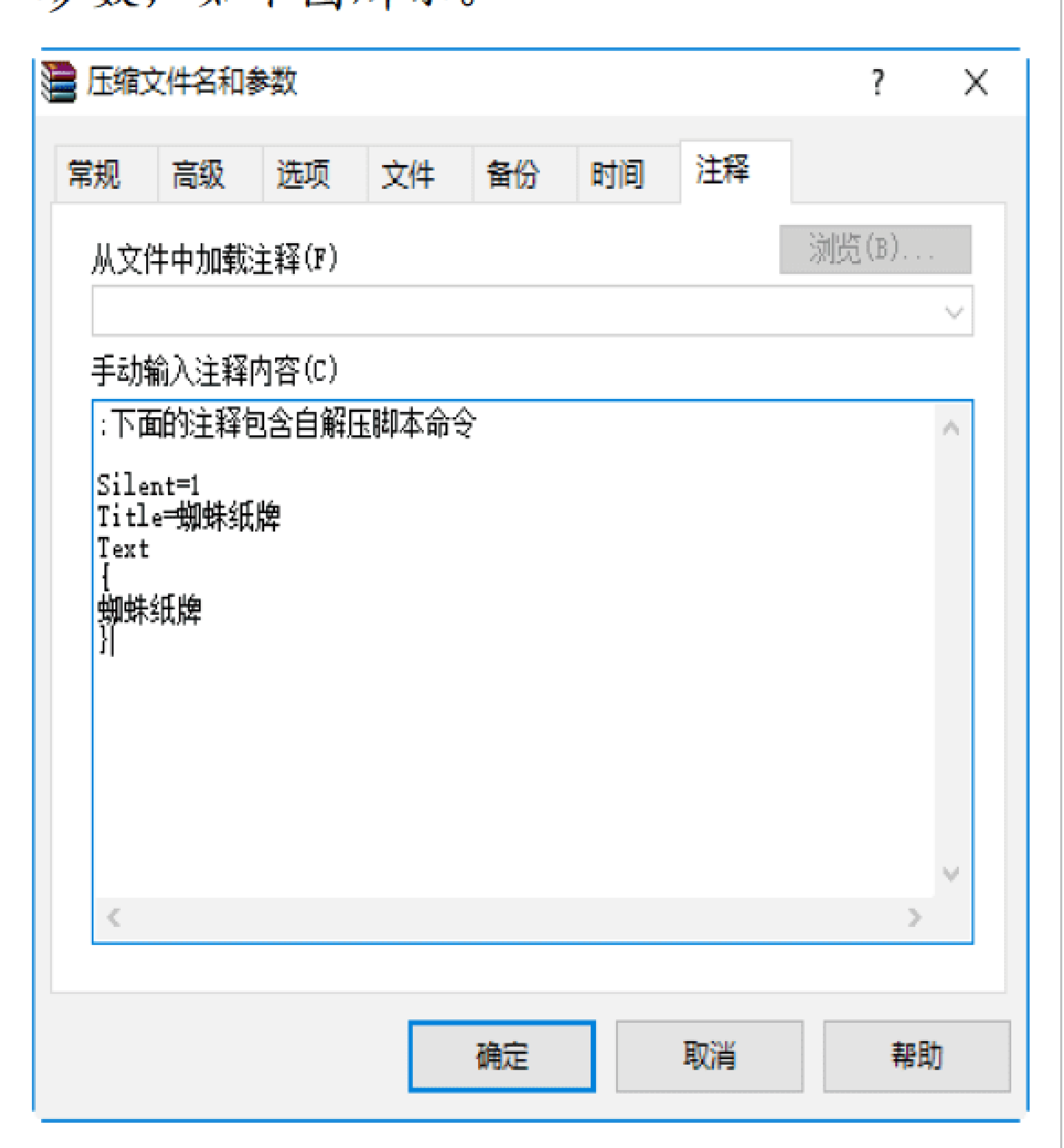
Step 06 选择“模式”选项卡，在其中选中“全部隐藏”单选按钮，这样可以增加木马程序的隐蔽性，如下图所示。

高级自解压选项
文本和图标 许可 模块
常规 设置 模式 高级 更新
临时模式
解包到临时文件夹(T)
可选的询问(Q)
询问标题(I)
安静模式
全部显示(A)
隐藏启动对话框(S)
全部隐藏(H)
确定 取消 帮助

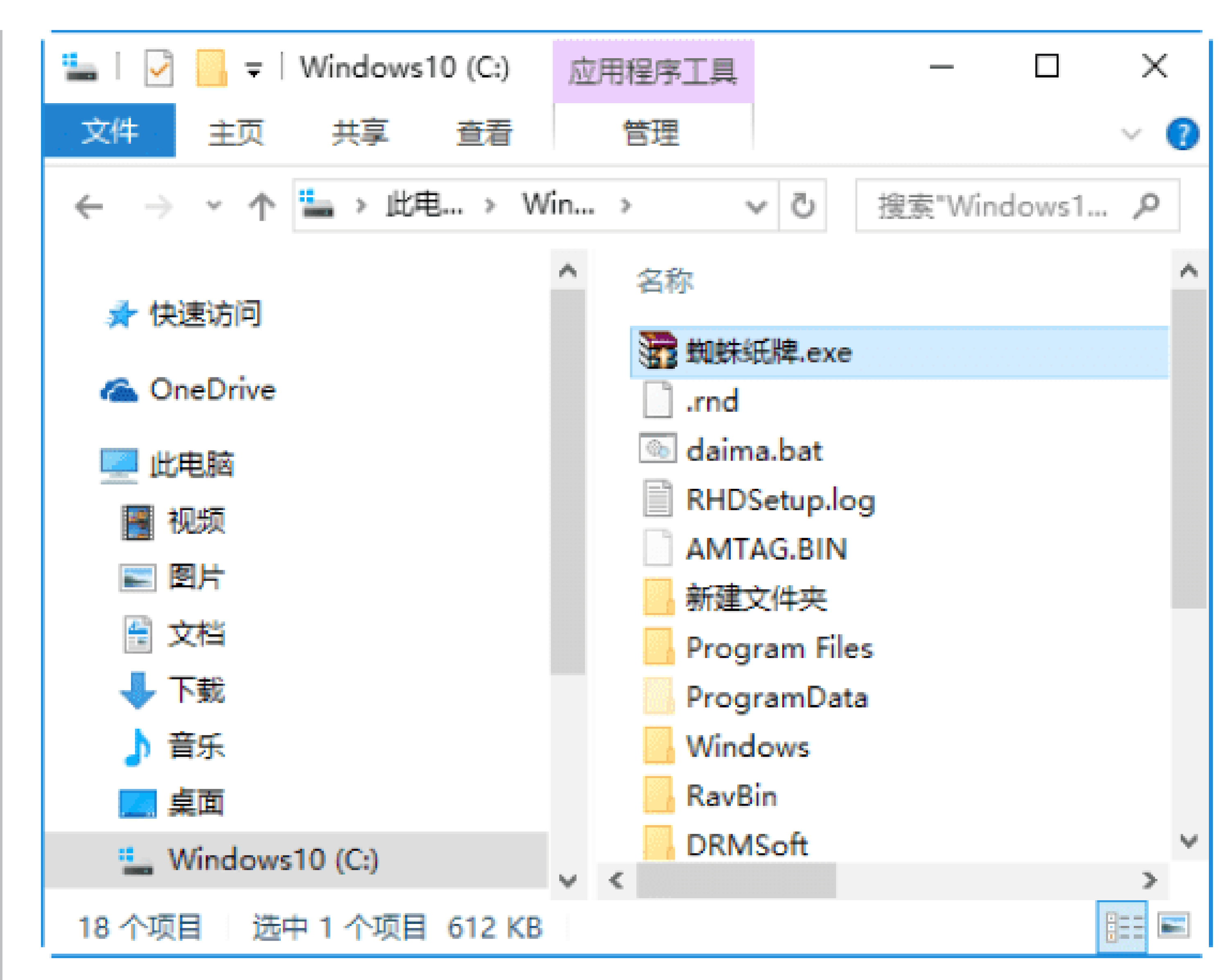
Step 07 为了更好地迷惑用户，还可以在“文本和图标”选项卡下设置自解压文件窗口标题、自解压文件图标等，如下图所示。



Step 08 设置完毕后，单击“确定”按钮，返回“压缩文件名和参数”对话框。在“注释”选项卡中可以看到自己所设置的各项参数，如下图所示。



Step 09 单击“确定”按钮，即可生成一个名为“蜘蛛纸牌”自解压的压缩文件，如下图所示。这样用户一旦运行该文件，就会中木马。



实战3：图片也可能是木马程序

将木马程序伪装成图片是许多木马制造者常用来骗别人执行木马的方法，如将木马伪装成GIF、JPG文件等，这种方式可以使很多人中招。用户可以使用“图片木马生成器”工具将木马伪装成图片。具体的操作步骤如下。

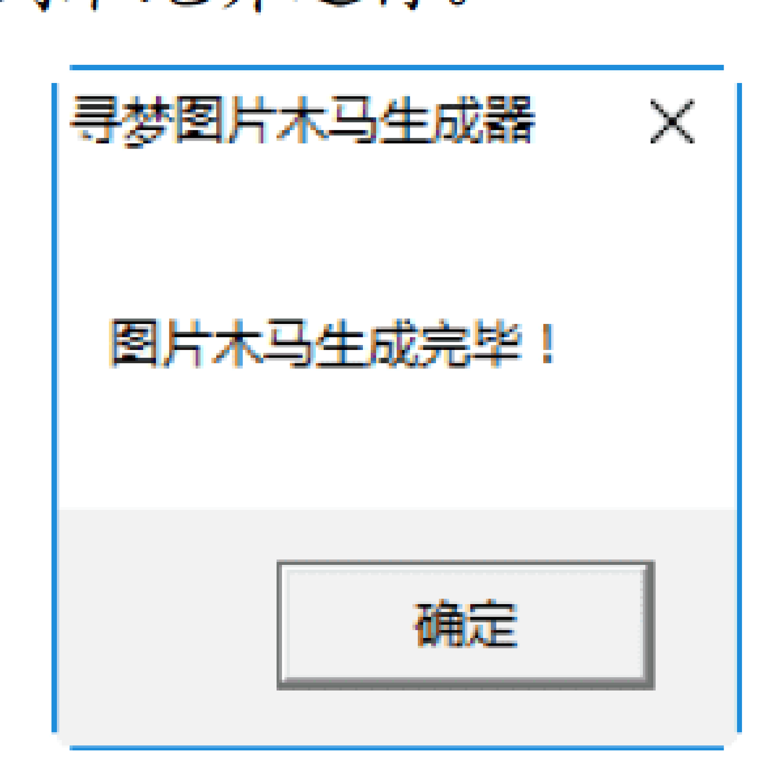
Step 01 下载并运行“寻梦图片木马生成器V1.0”程序，打开“寻梦图片木马生成器V1.0”主窗口，如下图所示。



Step 02 在“网页木马地址”和“真实图片地址”文本框中分别输入网页木马和真实图片地址；在“选择图片格式”下拉列表中选择.jpg选项，如下图所示。



Step 03 单击“生成”按钮，随即弹出“图片木马生成完毕！”提示框，如下图所示。单击“确定”按钮，关闭该提示框。这样只要打开该图片，就可以自动把该地址的木马下载到本地并运行。



4.3　使用木马清除软件清除木马

对于那些识别出来的木马程序，可以使用手工清除的方法将其删除，但是如果不了解发现的木马，要想确定木马的名称、入侵端口、隐藏位置和清除方法等都非常困难，这时就需要使用木马清除软件清除木马了。

实战4：使用《金山贝壳木马专杀》清除木马

《金山贝壳木马专杀》是国内首款专为网游防盗号量身打造的，完全免费的木马专杀软件。其安全检测采用云计算技术，拥有世界最大的云安全数据库，能在5分钟内快速识别新木马/病毒，保证系统、账号、用户隐私安全。

使用《金山贝壳木马专杀》清除木马的具体操作步骤如下。

Step 01 下载并安装《贝壳木马专杀1.5》软件，双击其快捷图标，打开“贝壳木马专杀1.5”主窗口，如下图所示。



Step 02 选中“快速扫描”单选按钮后，单击“开始查杀”按钮，即可开始查杀病毒。在“云安全检测”选项卡下即可看到信任文件、无威胁文件、未知文件、木马/病毒等类型文件的个数，如下图所示。



Step 03 在扫描的过程中，如果发现存在有木马病毒文件，将会弹出“发现木马”对话框，在其中显示木马的名称、路径等信息。用户可根据实际需要选择“清除”或“跳过”，这里单击“清除”按钮，即可清除该木马文件，如下图所示。



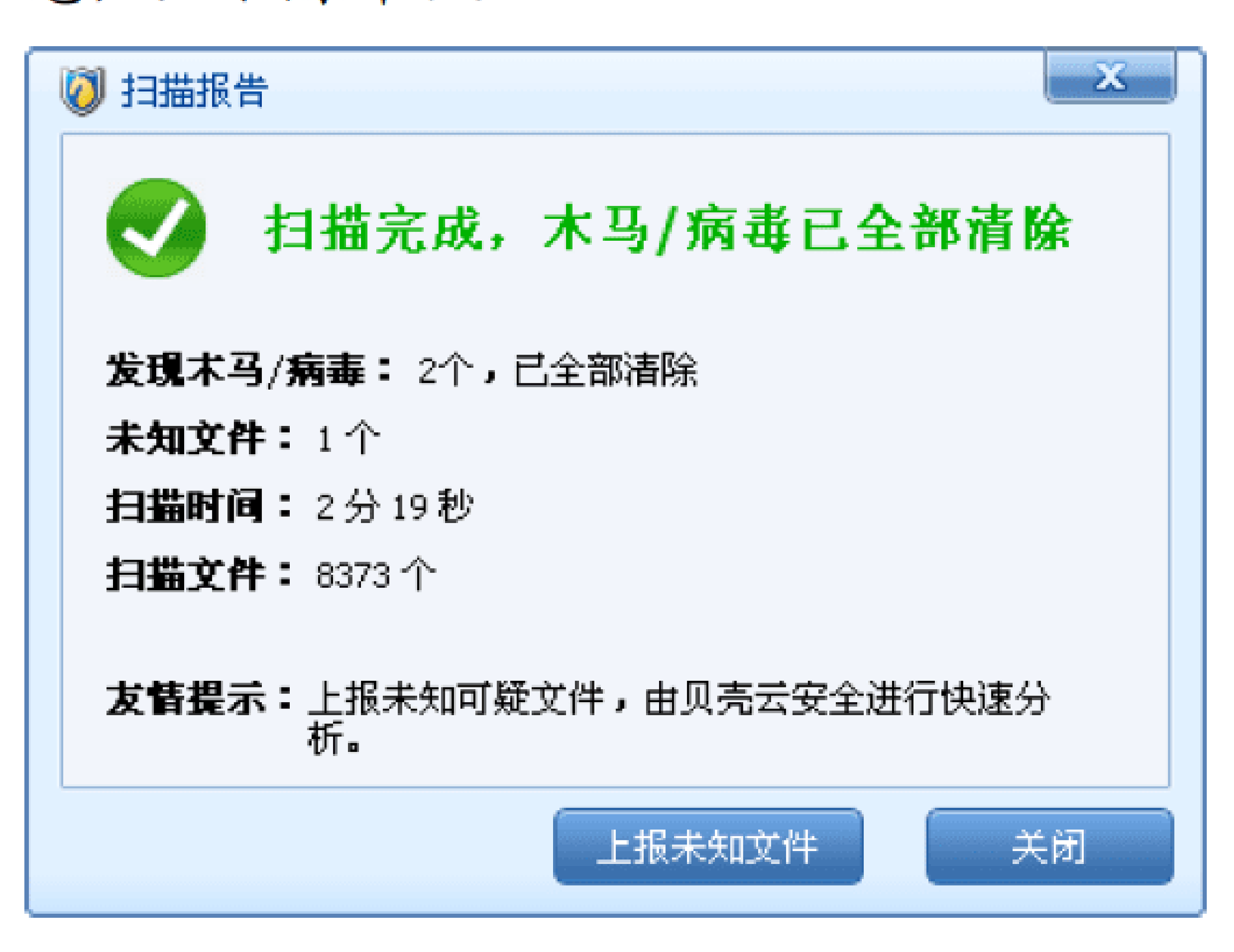


Step 04 如果想查看木马的详细信息，则可在“发现木马”对话框中单击“去病毒百科查看详情”超链接，打开“贝壳安全文件百科”窗口，在其中即可看到该病毒文件的详细信息，如下图所示。





Step 05 待扫描完成后，打开“扫描报告”对话框，在其中可查看发现的木马病毒数、扫描所用的时间以及扫描的文件数等信息，如下图所示。



Step 06 单击“关闭”按钮，返回到“贝壳木马专杀1.5”主界面，选择“木马/病毒”选项卡，在其中即可看到已经清除的木马病毒文件列表，如下图所示。



实战5：使用Spyware Doctor清除木马

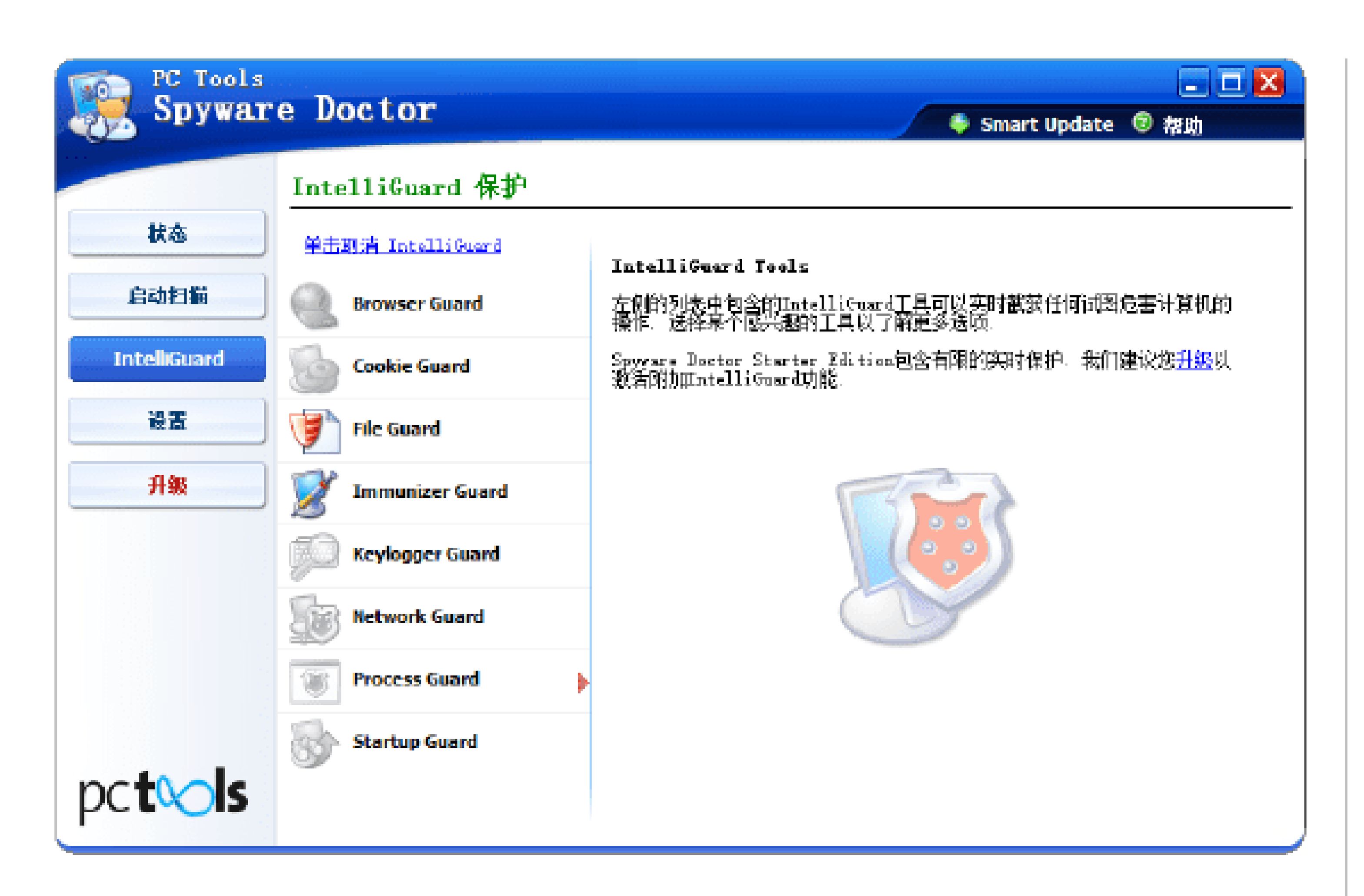
Spyware Doctor是一款非常先进的间谍软件、木马程序清除工具，可以检查并从计算机中移除间谍软件、广告软件、木马程序、键盘记录器和追踪威胁等。

使用Spyware Doctor清除木马程序的具体操作步骤如下。

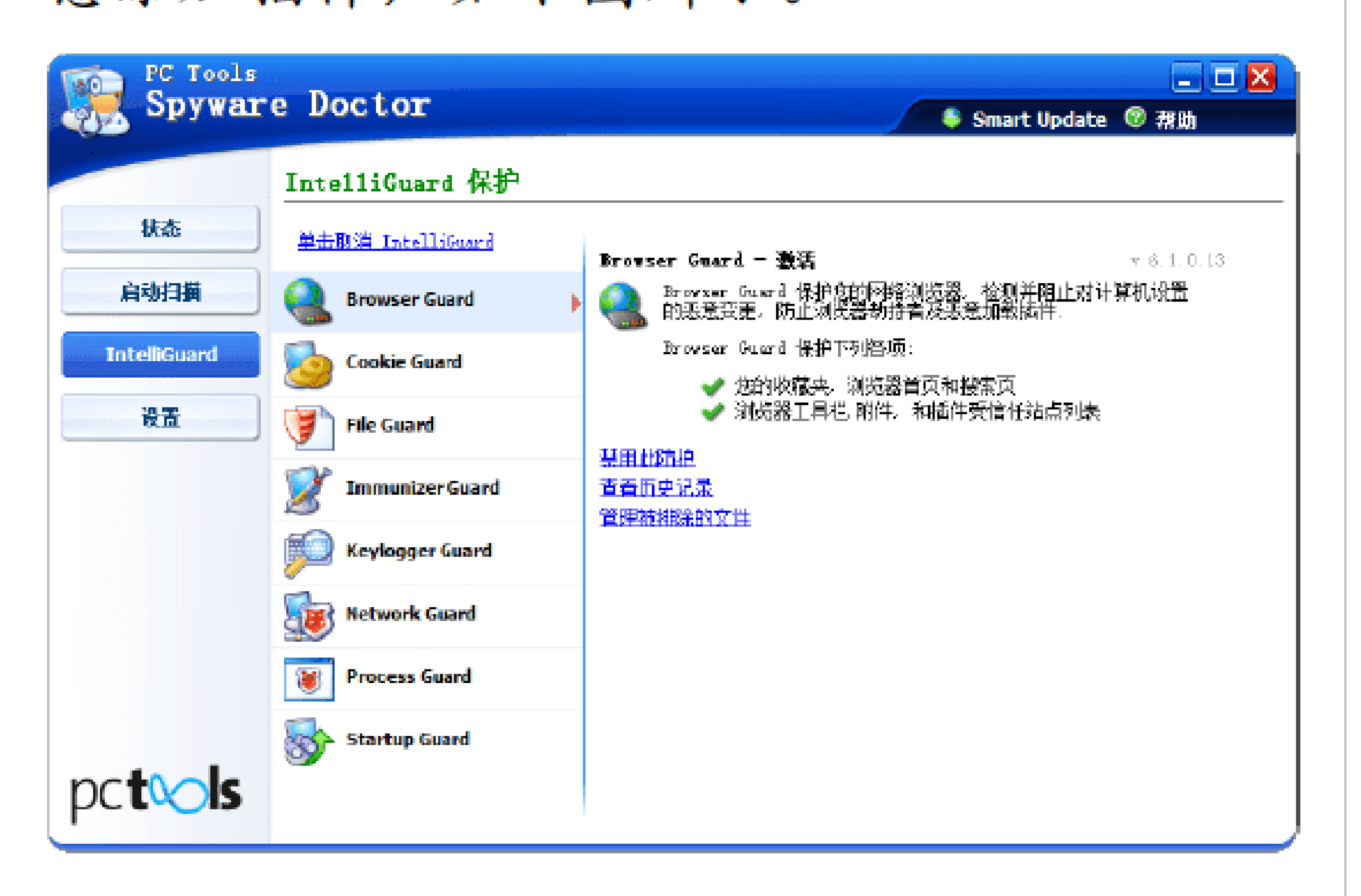
Step 01 下载并安装Spyware Doctor，双击桌面上的Spyware Doctor图标，打开Spyware Doctor窗口，如下图所示。



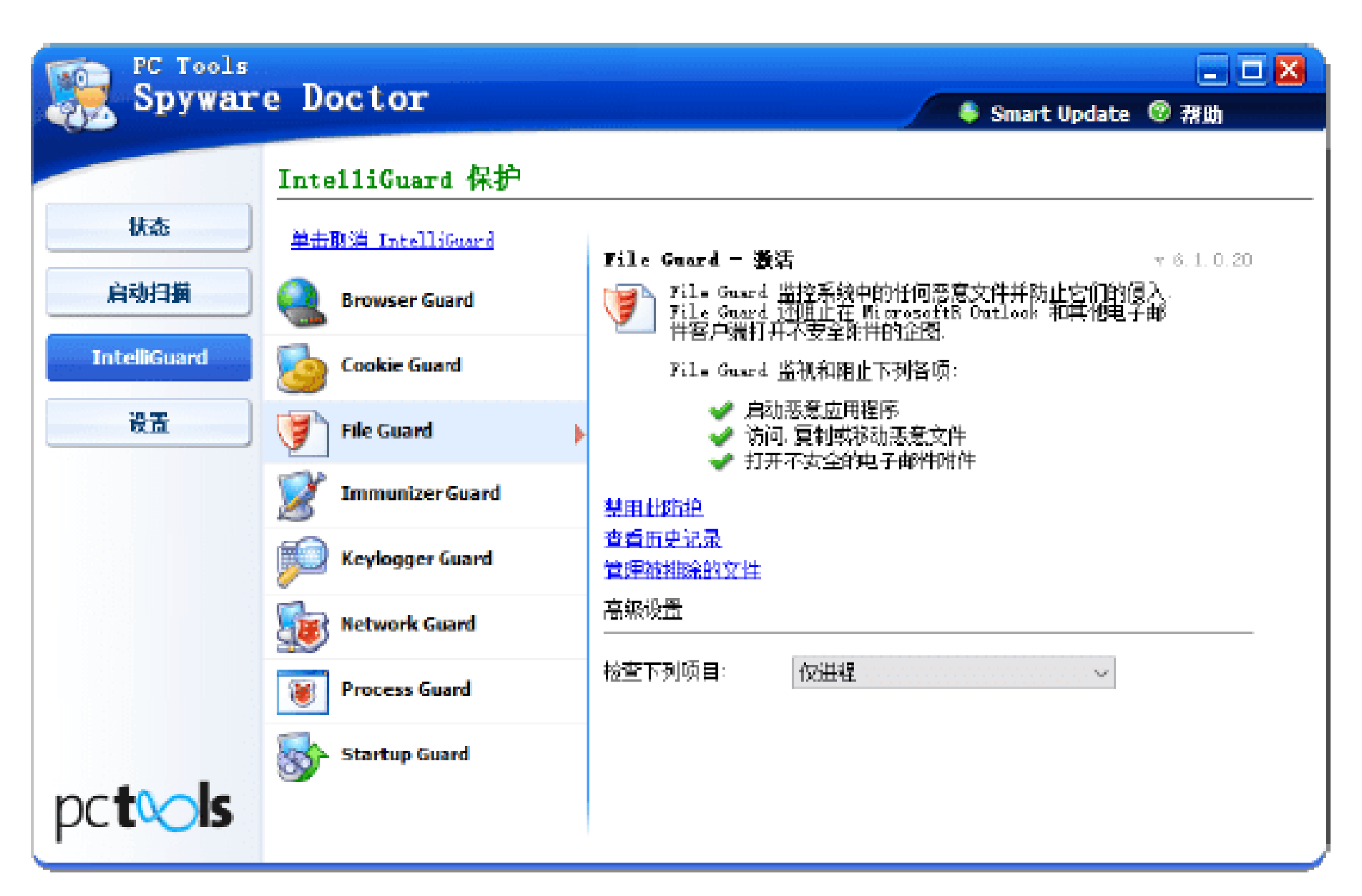
Step 02 在IntelliGuard选项卡中单击“单击激活IntelliGuard”链接，即可激活IntelliGuard，如下图所示。



Step 03 在Spyware Doctor窗口中单击Browser Guard选项，打开Browser Guard窗口，在其中设置Browser Guard参数，从而保护浏览器设置不被恶意变更，以防止浏览器被恶意添加插件，如下图所示。



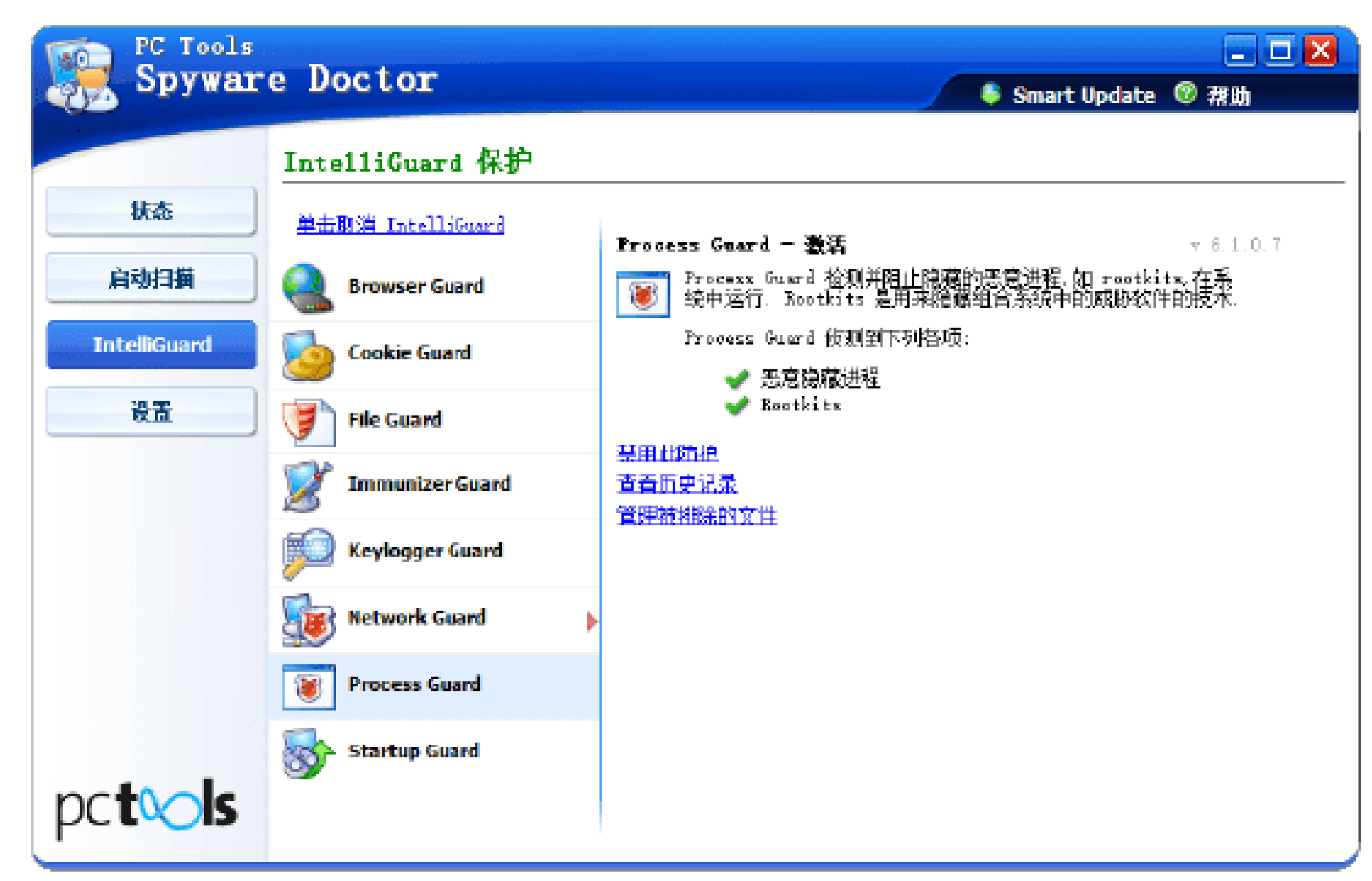
Step 04 单击File Guard选项，打开File Guard窗口，在其中设置File Guard参数，从而监控系统中的所有文件，以防止被入侵，如下图所示。



Step 05 单击Netword Guard选项，打开Netword Guard窗口，在其中设置Netword Guard参数，以阻止对网路设置的恶意更改，使得威胁软件停止拦截网络连接，如下图所示。



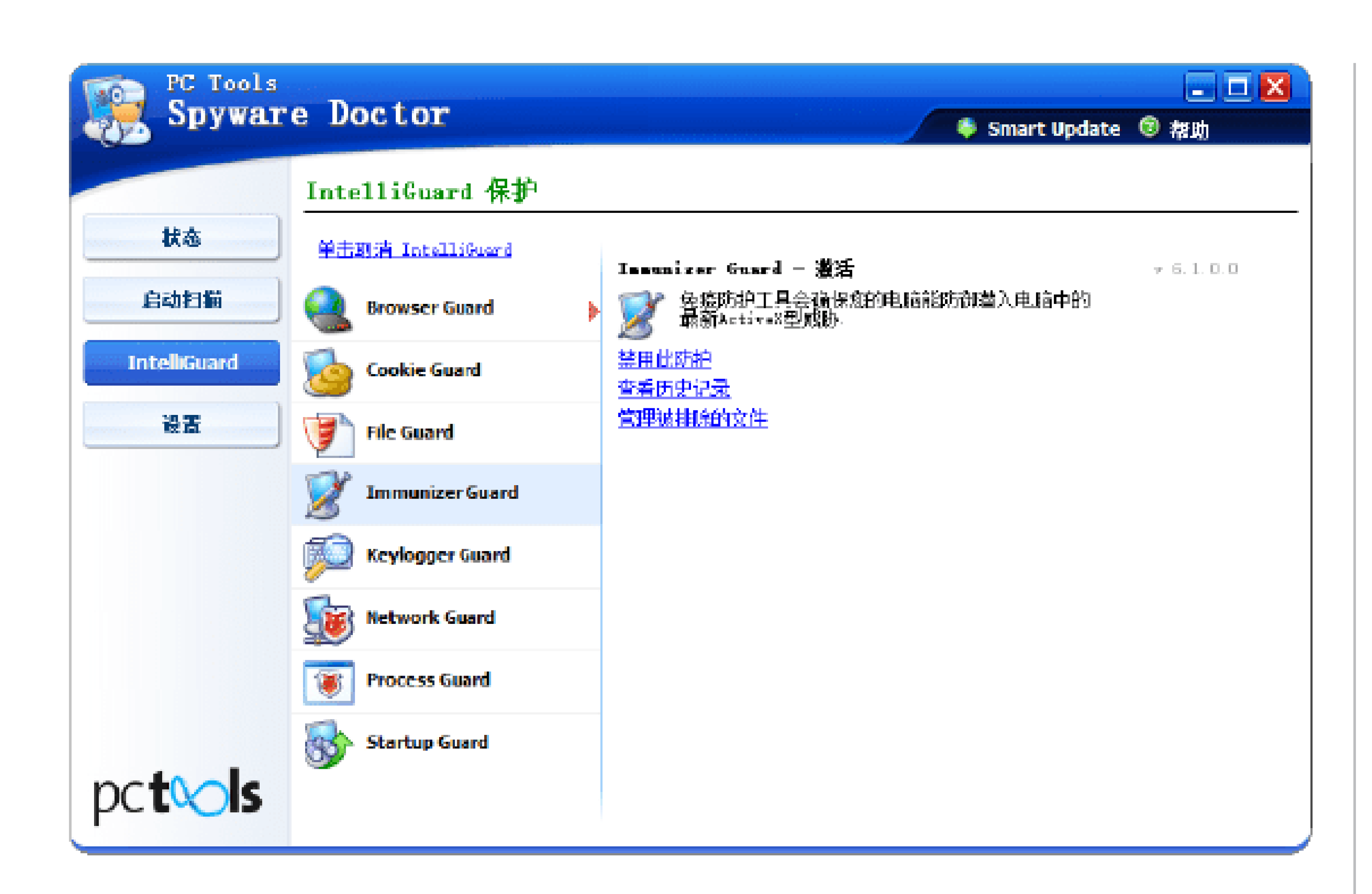
Step 06 单击Prrocess Guard选项，打开Process Guard窗口，在其中设置Prrocess Guard参数，以检测并阻止隐藏的恶意进程，如下图所示。



Step 07 单击Startup Guard选项，打开Startup Guard窗口，在其中设置Startup Guard参数，以检测并阻止恶意应用软件在系统中的配置并自动启动，如下图所示。



Step 08 单击Immunizer Guard选项，打开Immunizer Guard窗口，在其中设置Immunizer Guard参数，以防御嵌入计算机中最新ActiveX型威胁，如下图所示。



Step 09 单击Cookie Guard选项，打开Cookie Guard窗口，在其中设置Cookie Guard参数，以监视浏览器是否存在恶意跟踪或广告，如下图所示。



Step 10 单击“设置”按钮，打开“常规设置”窗口，在其中定义Spyware Doctor的常规设置，如下图所示。



Step 11 单击“高级”选项，打开“高级设置”窗口，在其中定义Spyware Doctor高级设置参数，如下图所示。



Step 12 单击“扫描设置”选项，打开“扫描设置”窗口，在其中定义防间谍软件和防病毒的扫描设置参数，如下图所示。



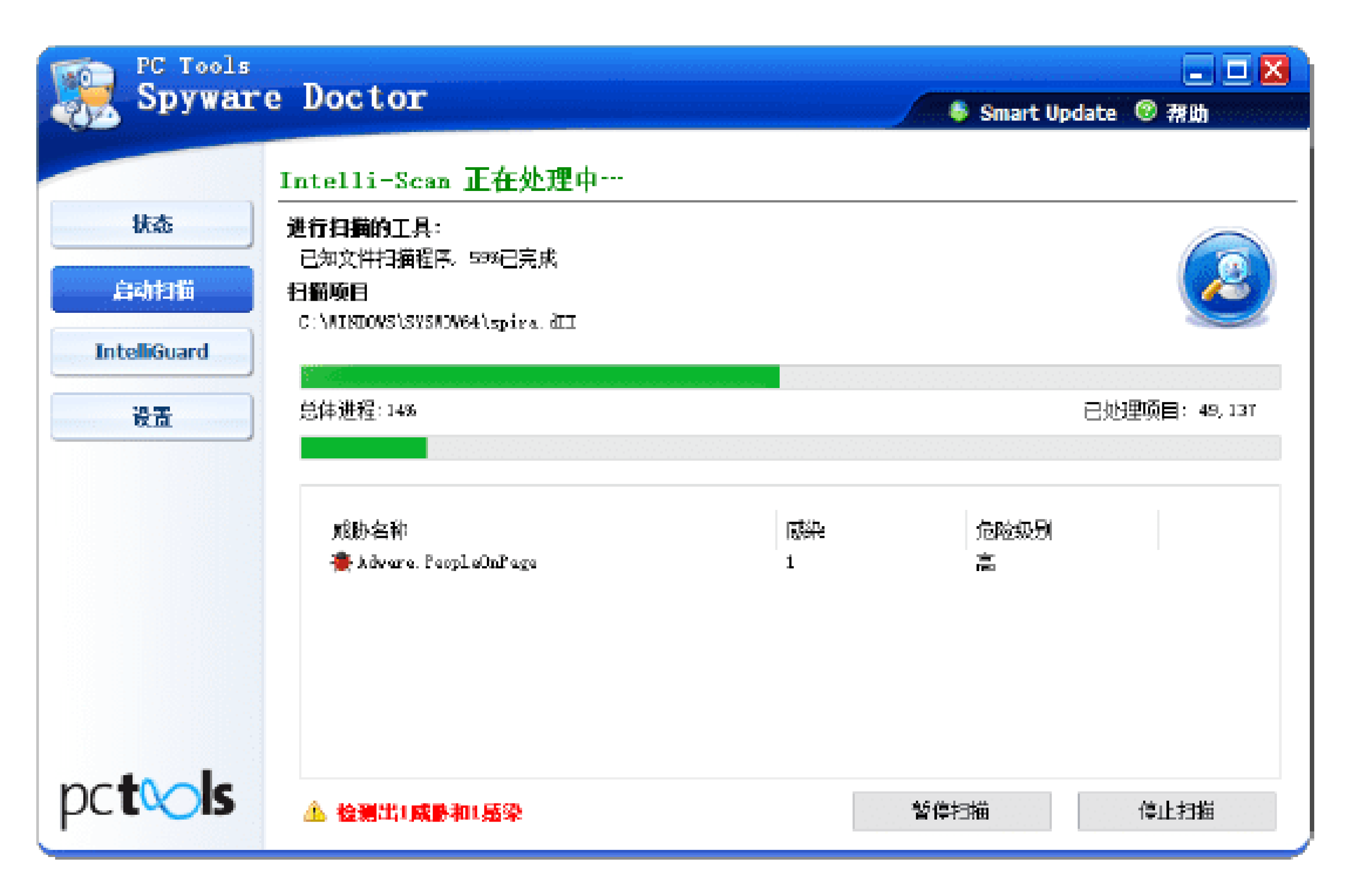
Step 13 单击“计划任务”选项，打开“计划任务”窗口，在其中可以添加扫描计划任务，即在特定的时间运行各类自动运行任务，如下图所示。



Step 14 单击“隔离”选项，打开“隔离”窗口，在其中可以查看被隔离的项目，如下图所示。



Step 15 单击“启动扫描”按钮，即可开始进行扫描，并显示扫描的进度，如下图所示。



Step 16 在等待扫描完毕之后，就会弹出“扫描结果”对话框，在其中显示扫描出来的危险项目。单击“选定修复项”按钮，即可自动处理扫描出来的危险项目，如下图所示。



4.4　使用《360杀毒》软件查杀病毒

当计算机出现了中毒后的特征后，就需要对其查杀病毒。流行的杀毒软件很多，360杀毒是使用比较广泛的杀毒软件之一，该软件引用双引擎的机制，拥有完善的病毒防护体系，不但查杀能力出色，而且对于木马病毒能够第一时间进行防御。

实战6：安装《360杀毒》软件



《360杀毒》软件下载完成后，即可进行安装。具体操作步骤如下。

Step 01 双击下载的《360杀毒5.0》软件安装程序，即可打开如下图所示的安装界面。



Step 02 单击“立即安装”按钮，即可开始安装《360杀毒》软件，并显示安装的进度，如下图所示。



Step 03 安装完毕后，弹出360新版特性提示对话框，如下图所示。



Step 04 单击“立即体验”按钮，即可打开360杀毒主界面，从而完成360杀毒的安装，如下图所示。



实战7：升级《360杀毒》的病毒库

病毒库其实就是一个数据库，里面记录着计算机病毒的种种特征，以便及时发现病毒并绞杀它们。只有拥有了病毒库，杀毒软件才能区分病毒和普通程序之间的区别。不过，要想让计算机能够对新病毒有所防御，就必须保证本地杀毒软件的病毒库一直处于最新版本。下面以《360杀毒》的病毒库升级为例进行介绍，具体操作步骤如下。

Step 01 单击360杀毒主界面的“检查更新”链接，如下图所示。



Step 02 弹出“360杀毒-升级”对话框，提示用户正在升级，并显示升级的进度，如下图所示。



Step 03 升级完成后，弹出“360杀毒-升级”对话框，提示用户“升级成功完成”，并显示程序的版本等信息，如下图所示。



Step 04 单击病毒库日期右侧的“立即开启”按钮，开始升级病毒库信息，如下图所示。



Step 05 升级完成后，提示用户“常规引擎已成功安装”，如下图所示。



Step 06 单击“查看升级日志”超链接，即可打开“360杀毒-日志”对话框，在其中显示产品升级的记录，如下图所示。



实战8：快速查杀计算机中的病毒

一旦发现计算机运行不正常，用户首先分析原因，然后即可利用杀毒软件进行杀毒操作。下面以《360杀毒》查杀病毒为例，讲解如何利用杀毒软件杀毒。

使用《360杀毒》软件杀毒的具体操作步骤如下。

Step 01 启动360杀毒，360杀毒为用户提供了3种查杀病毒的方式，即快速扫描、全盘扫描和自定义扫描，如下图所示。



Step 02 这里选择快速扫描方式，单击“快速扫描”按钮，即可开始扫描系统中病毒文件，如下图所示。



Step 03 在扫描的过程中，如果发现木马病毒，则会在下面的空格中显示扫描出来的木马病毒，并列出其危险程度和相关描述信息。





Step 04 单击“立即处理”按钮，即可删除扫描出来的木马病毒或安全威胁对象，如下图所示。



Step 05 单击“确定”按钮，返回到“360杀毒”窗口，在其中显示被360杀毒处理的项目，如下图所示。



Step 06 单击“隔离区”超链接，打开“360恢复区”对话框，在其中显示被360杀毒处理的项目，如下图所示。

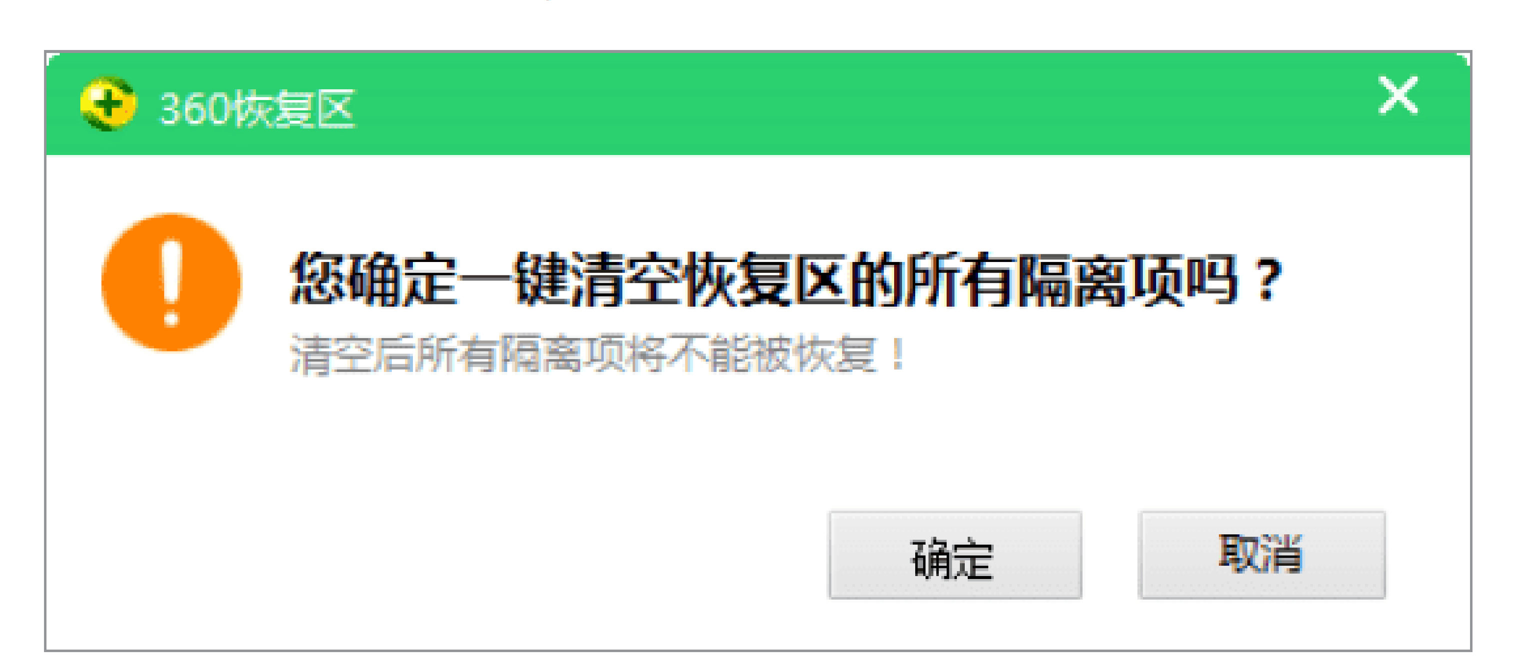


Step 07 勾选“全选”复选框，选中所有恢复区的项目，如下图所示。

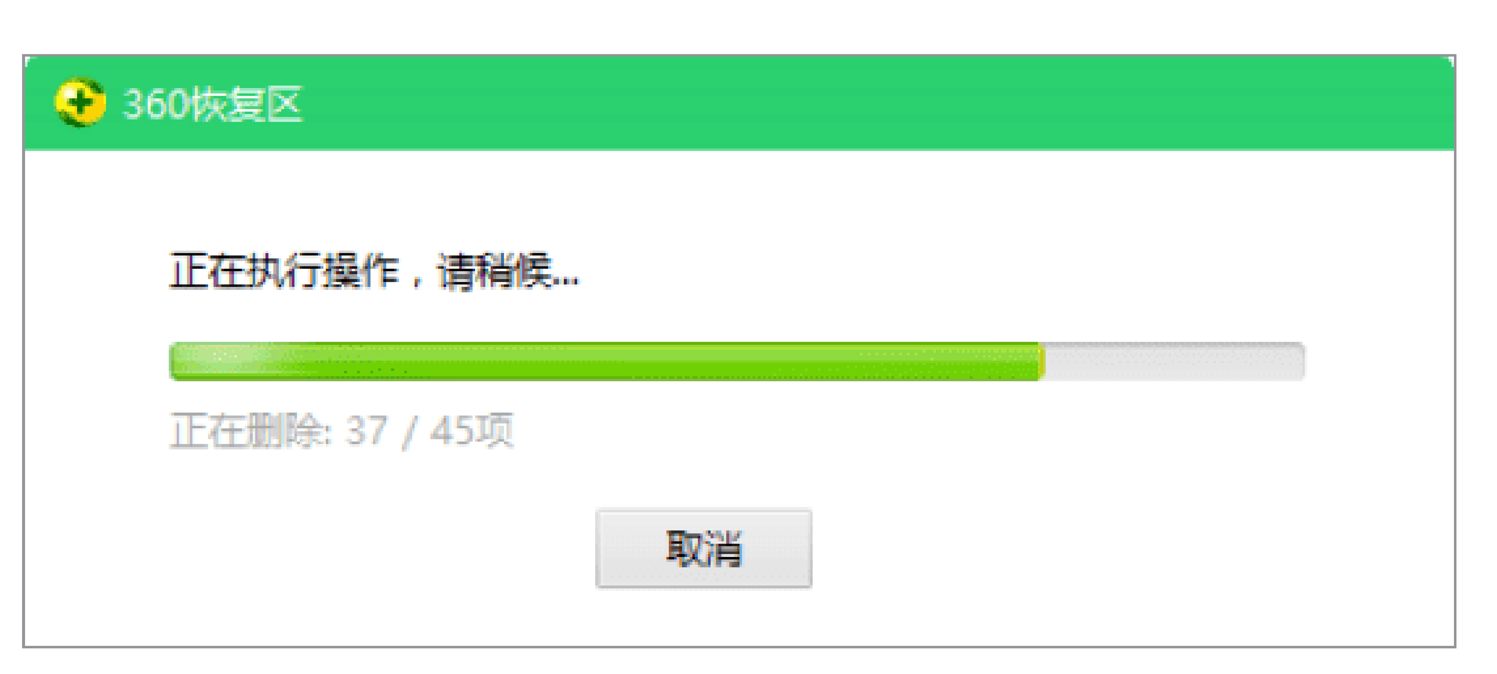




Step 08 单击“清空恢复区”按钮，弹出一个信息提示框，提示用户是否确定要一键清空恢复区的所有隔离项，如下图所示。



Step 09 单击“确定”按钮，即可开始清除恢复区所有的项目，并显示清除的进度，如下图所示。



Step 10 清除恢复区所有项目完毕后，将返回“360恢复区”对话框，如下图所示。



另外，使用360杀毒还可以对系统进行全盘杀毒。只需在“病毒查杀”选项卡下单击“全盘扫描”按钮即可，全盘扫描和快速扫描类似，这里不再详述。

实战9：自定义查杀计算机中的病毒

下面介绍一下如何对指定位置进行病毒的查杀，具体的操作步骤如下。

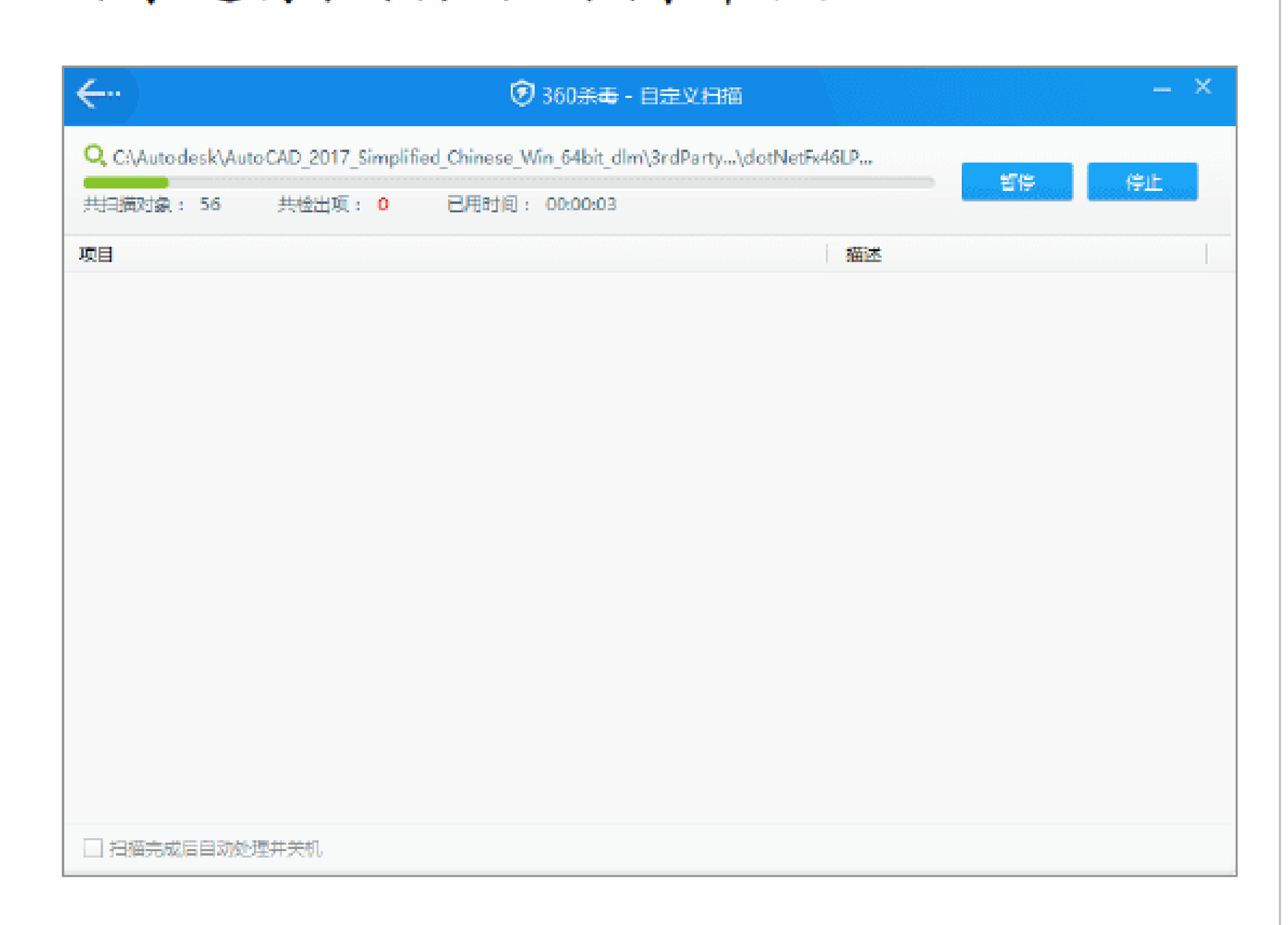
Step 01 在360杀毒工作界面中单击“自定义扫描”图标，如下图所示。



Step 02 打开“选择扫描目录”对话框，在需要扫描的目录或文件前勾选相应的复选框，这里勾选Windows 10（C）复选框，如下图所示。



Step 03 单击“扫描”按钮，即可开始对指定目录进行扫描，如下图所示。



其余步骤和“快速查杀”相似，不再详细介绍。

提示： 大部分杀毒软件查杀病毒的方法比较相似，用户可以利用自己的杀毒软件进行类似的病毒查杀操作。

4.5　使用病毒专杀工具查杀病毒

在使用杀毒软件查杀病毒的过程中，一些比较顽固的病毒是扫描不出来的，这时就需要使用一些专门的病毒查杀工具来查杀计算机病毒了。

实战10：查杀异鬼病毒

异鬼病毒是腾讯计算机管家捕获的一恶性Bootkit病毒，该病毒可篡改浏览器主页、劫持导航网站，并在后台刷取流量。不过，计算机管家已全面防御“异鬼Ⅱ”病毒，使用计算机管家查杀“异鬼Ⅱ”病毒的操作步骤如下。

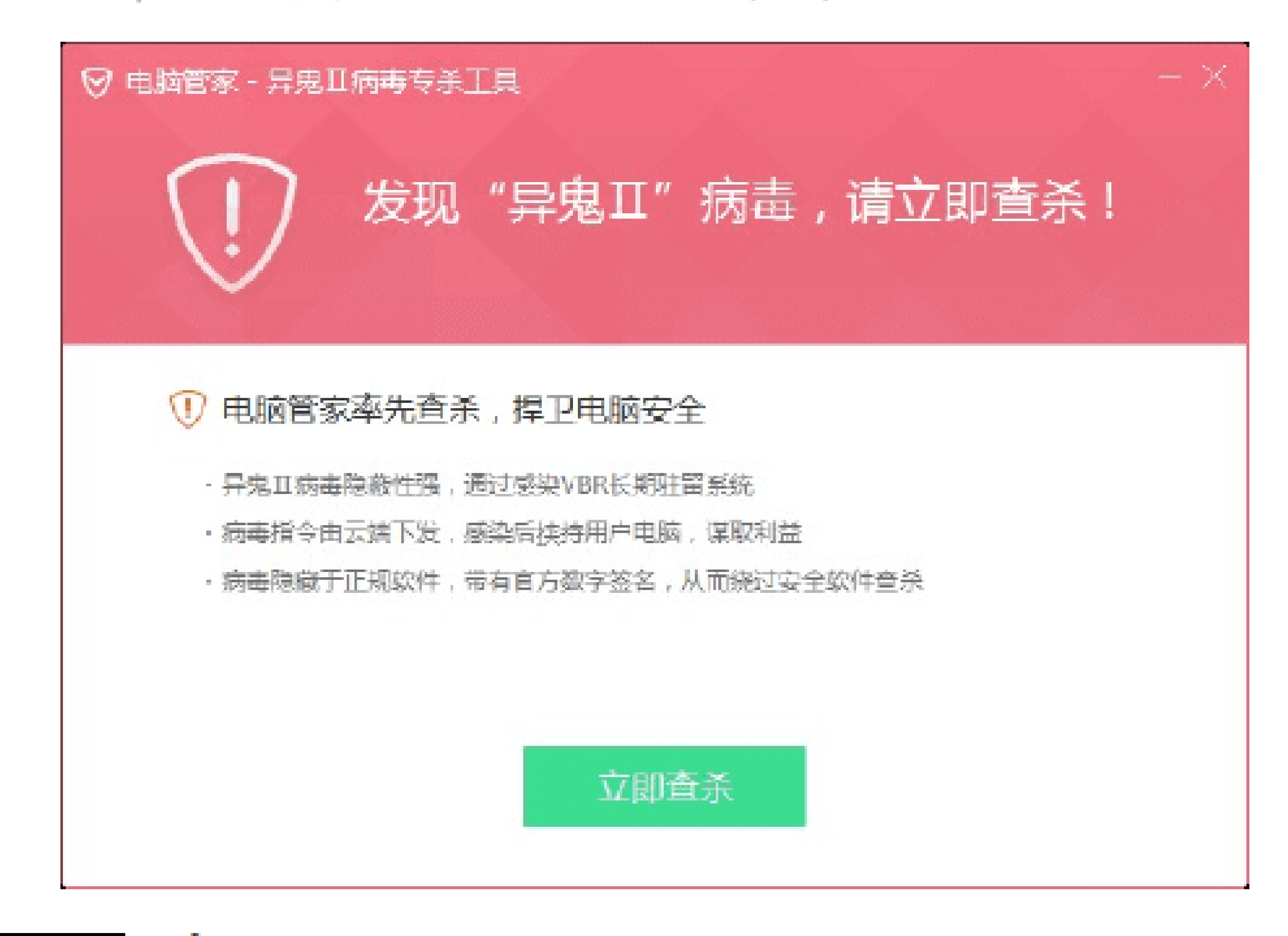
Step 01 在计算机管家中下载“异鬼Ⅱ”病毒免疫工具，双击运行工具，即可进行开始扫描“异鬼Ⅱ”病毒，如下图所示。



Step 02 如果扫描过程中没有发现“异鬼Ⅱ”病毒，将给出计算机安全的信息提示，如下图所示。



Step 03 如果发现“异鬼Ⅱ”病毒，将给出计算机中存在异鬼病毒的信息提示，需要用户立即进行查杀，如下图所示。





Step 04 单击“立即查杀”按钮，即可开始查杀“异鬼Ⅱ”病毒，如下图所示。



Step 05 查杀完成后，将给出“异鬼Ⅱ”病毒已成功清除的信息提示，如下图所示。





实战11：查杀CAD病毒

CAD病毒是利用Lisp语言编写，在CAD启动时自动加载，并自动生成扩展名为.sp、.fans的程序，该病毒到处传播，致使许多杀毒软件也无能为力，甚至重装CAD也不能解决问题。360 CAD专杀工具是一款针对CAD病毒设计的查杀软件，专门查杀CAD病毒，让用户的计算机得到最佳保护。

Step 01 双击下载的360CAD病毒专杀工具，打开“360CAD病毒专杀工具”工作界面，如下图所示。





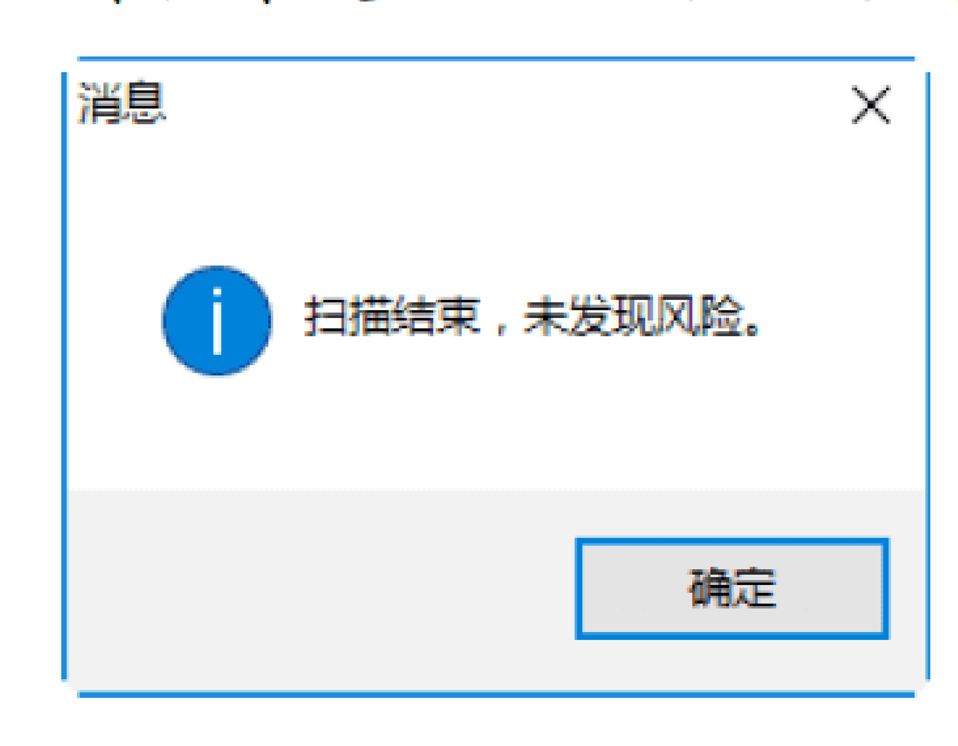
Step 02 单击“需扫描的分区”右侧的“所有分区”按钮，在弹出的下拉列表中选择需要扫描的分区，如下图所示。



Step 03 单击“开始扫描”按钮，即可开始扫描分区中存在的CAD病毒，对于扫描出来的CAD病毒，将直接进行查杀，如下图所示。



Step 04 扫描完成后，如果没有发现CAD病毒，将弹出“消息”对话框，提示用户“扫描结束，未发现风险”，如下图所示。



实战12：查杀U盘病毒

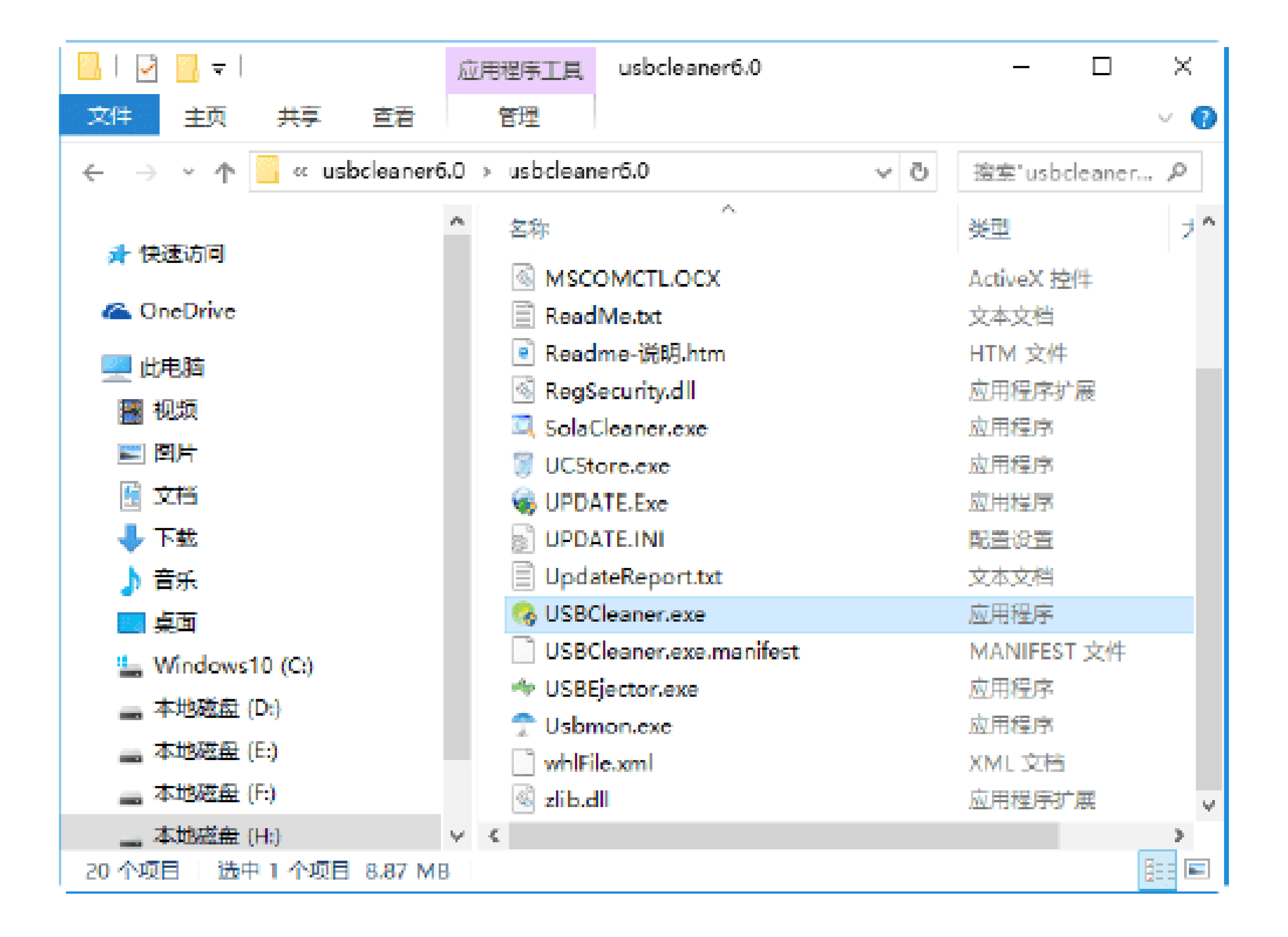
USBCleaner是一款绿色的辅助杀毒工具，具有检测查杀U盘病毒、U盘病毒广谱扫描、U盘病毒免疫、修复显示隐藏文件及系统文件、安全卸载移动盘等功能，可以

全方位一体化修复并查杀U盘病毒。

使用USBCleaner查杀病毒的具体操作步骤如下。

1.全面检测系统

Step 01 从网上下载U盘专杀工具，其文件夹中包含的文件，如下图所示。



Step 02 双击USBCleaner.exe图标，打开“U盘病毒专杀工具USBCleanerV6.0”对话框，如下图所示。



Step 03 单击“全面检测”按钮，即可对系统进行扫描，如下图所示。



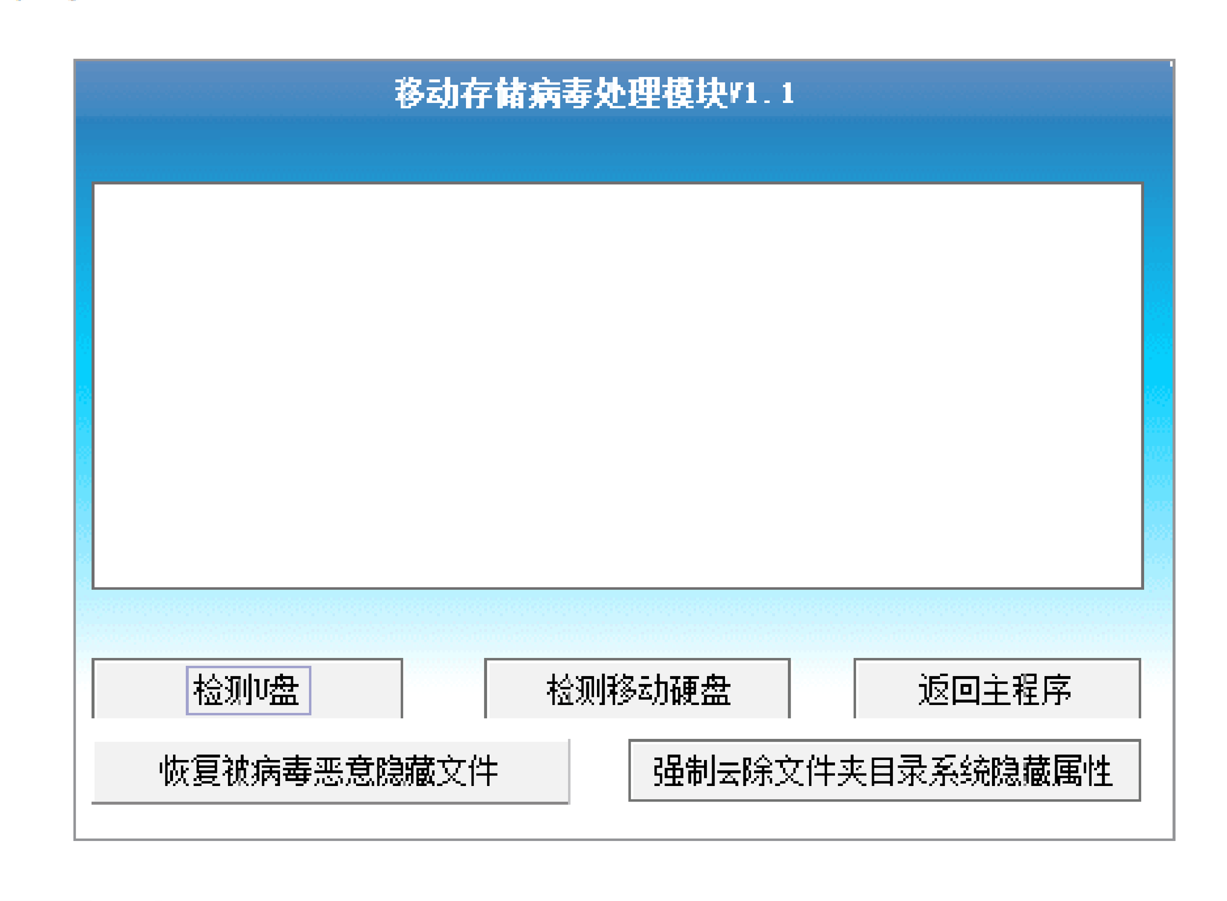
Step 04 在扫描的过程中，如果发现病毒，则会在下面的列表中显示，包括病毒的名称、文件路径和处理状态，如下图所示。



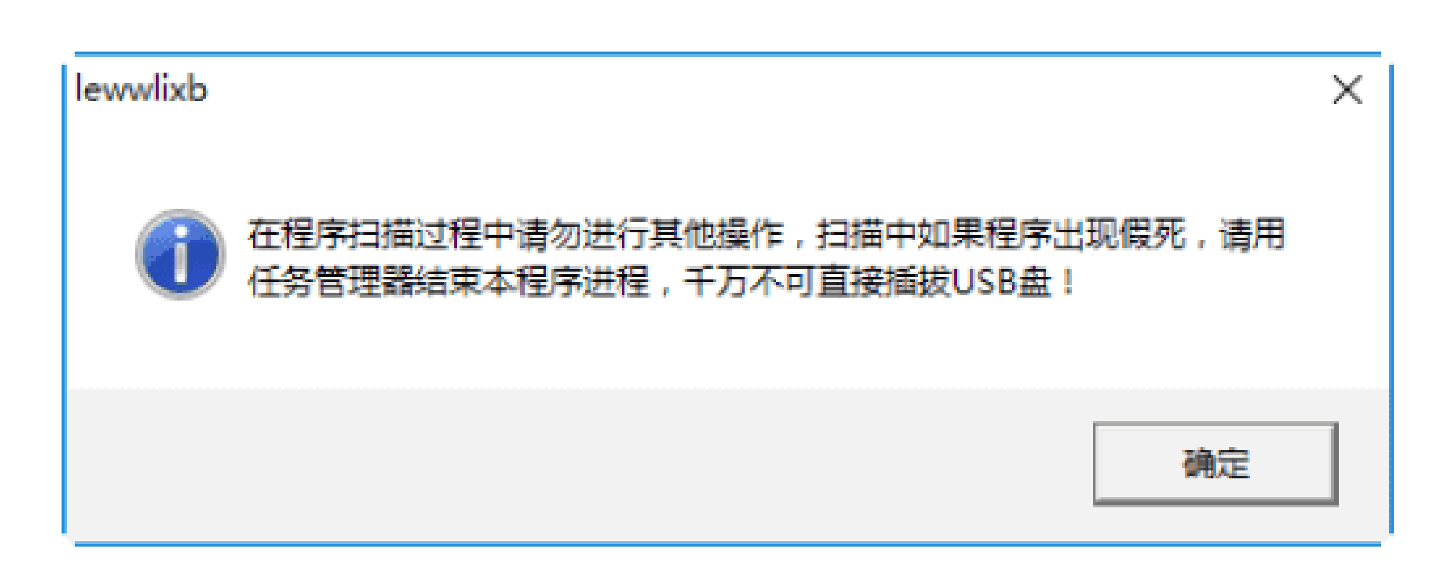
2.检测移动盘

具体的操作步骤如下。

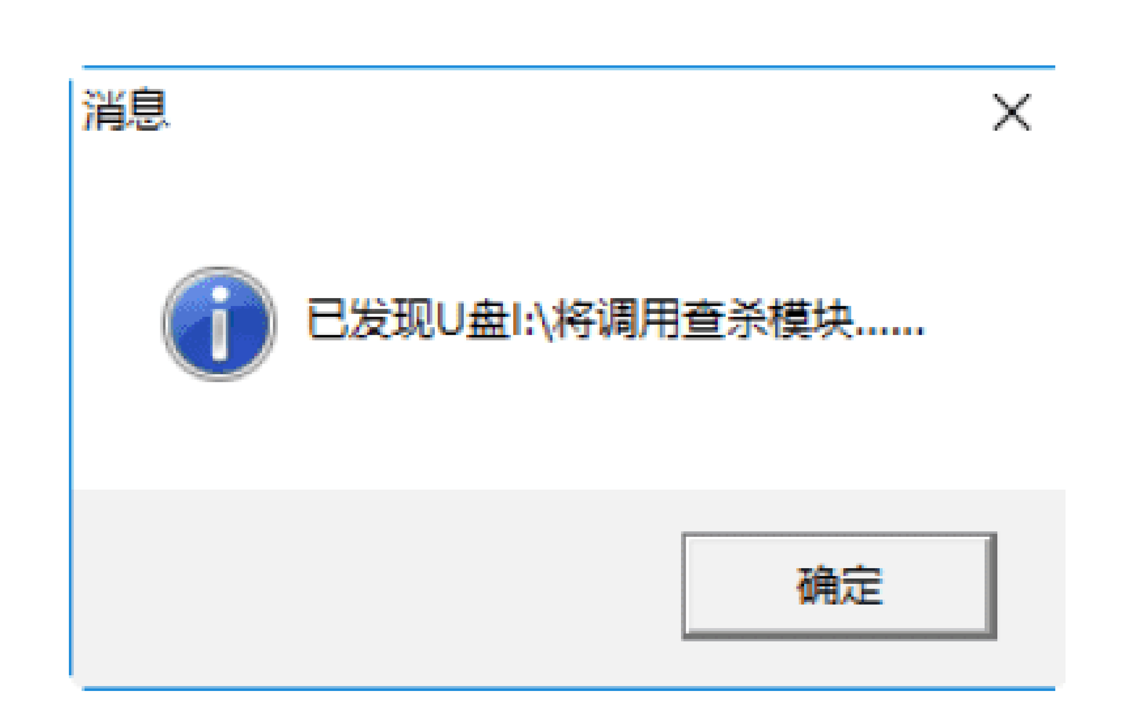
Step 01 单击“检测移动盘”按钮，打开“移动存储病毒处理模块V1.1”对话框，如下图所示。



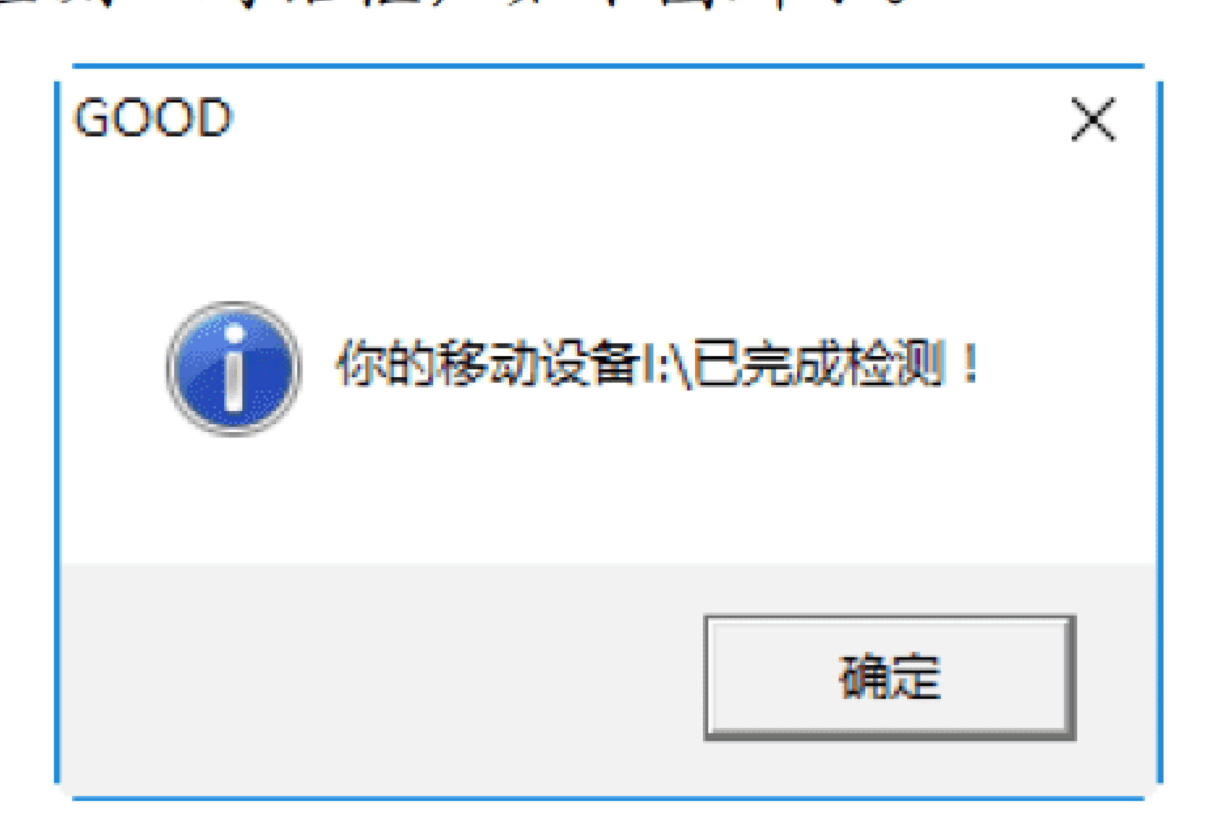
Step 02 单击“检测U盘”按钮，打开“千万不可直接插拔USB盘”提示框，如下图所示。



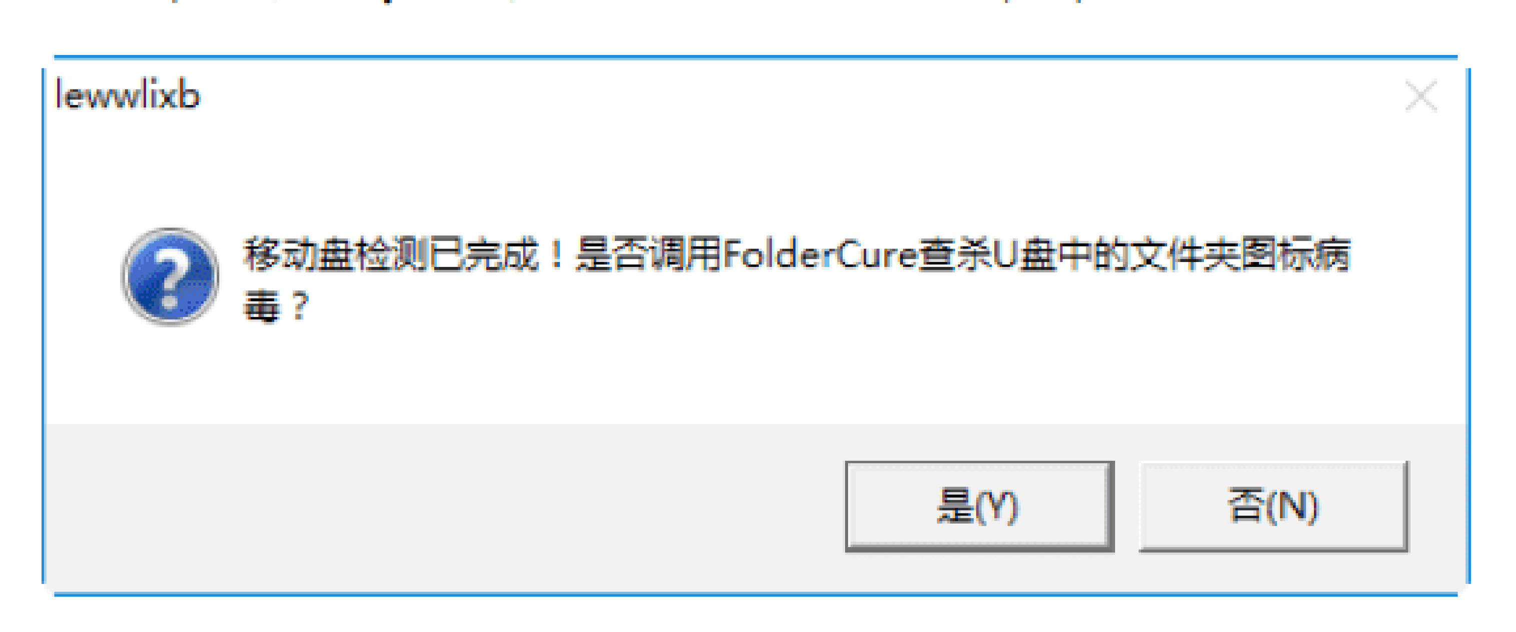
Step 03 单击“确定”按钮，打开“已发现U盘”信息提示框，如下图所示。



Step 04 单击“确定”按钮，即可对本机中的U盘进行检测，待检测完毕后，弹出“已完成检测”对话框，如下图所示。



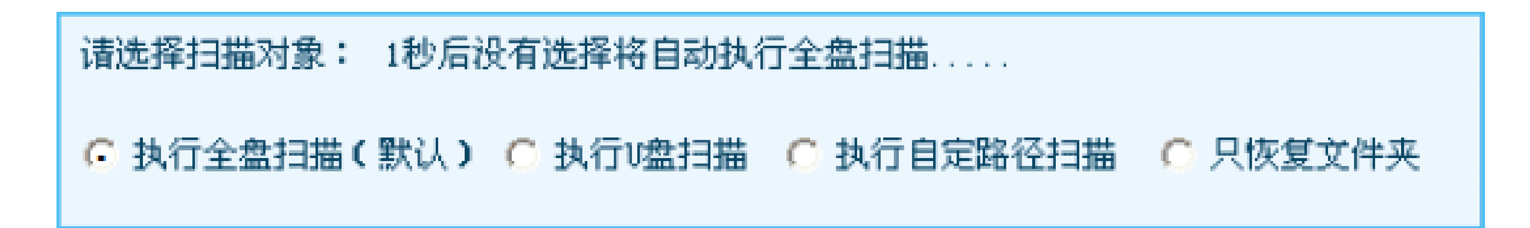
Step 05 单击“确定”按钮，打开“已完成检测，是否调用FolderCure查杀U盘中的文件夹图标病毒”提示框，如下图所示。



Step 06 单击“是”按钮，打开用USBCleaner中自带的“文件夹图标病毒专杀工具FolderCure”对话框，检测文件夹图标病毒，如下图所示。



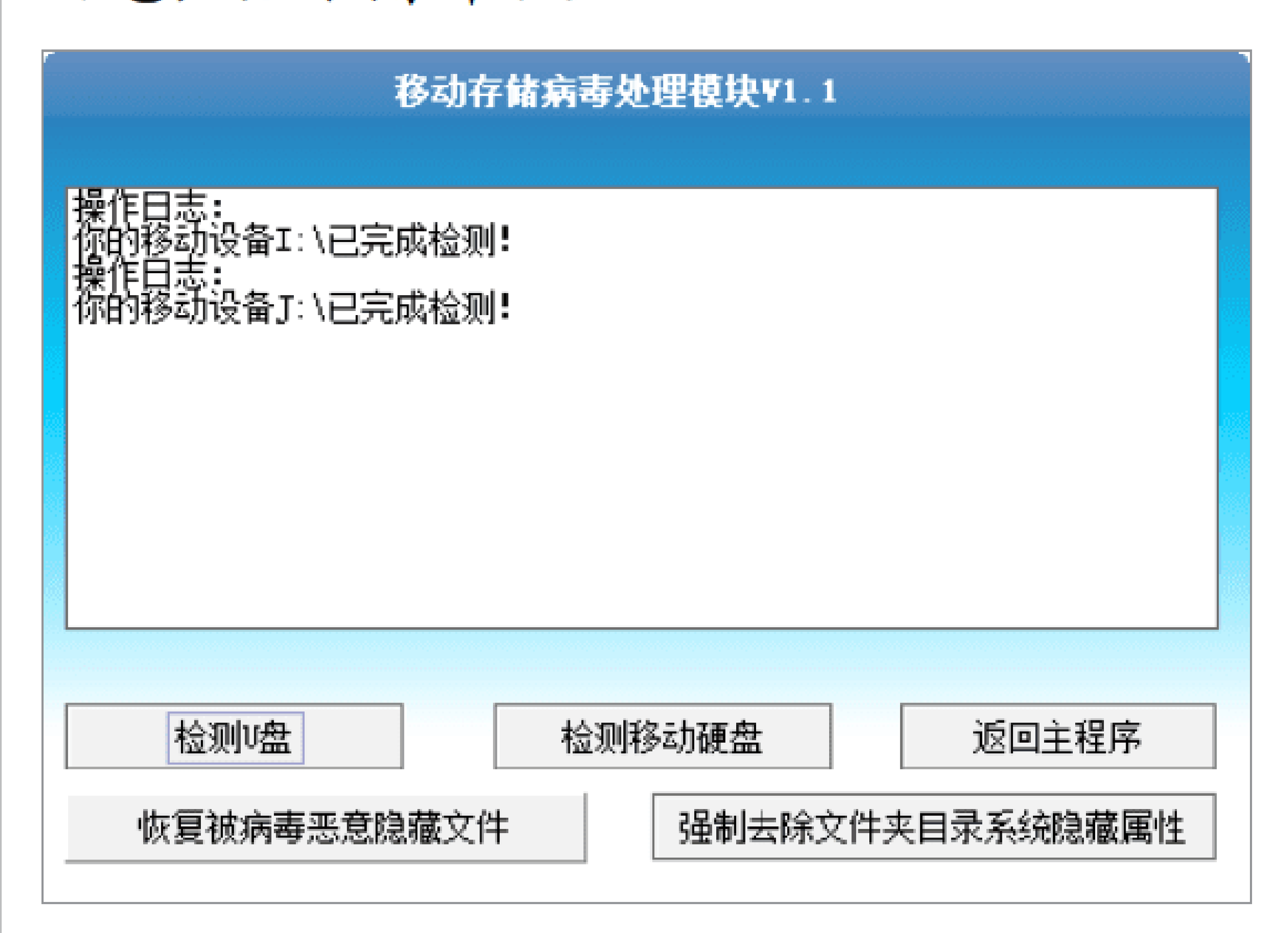
Step 07 单击“开始扫描”按钮，弹出“请选择扫描对象”信息提示。这里采用系统默认设置，即“执行全盘扫描（默认）”选项，如下图所示。



Step 08 选择完毕后，即可对系统中的全盘进行文件夹图标病毒的扫描，如下图所示。

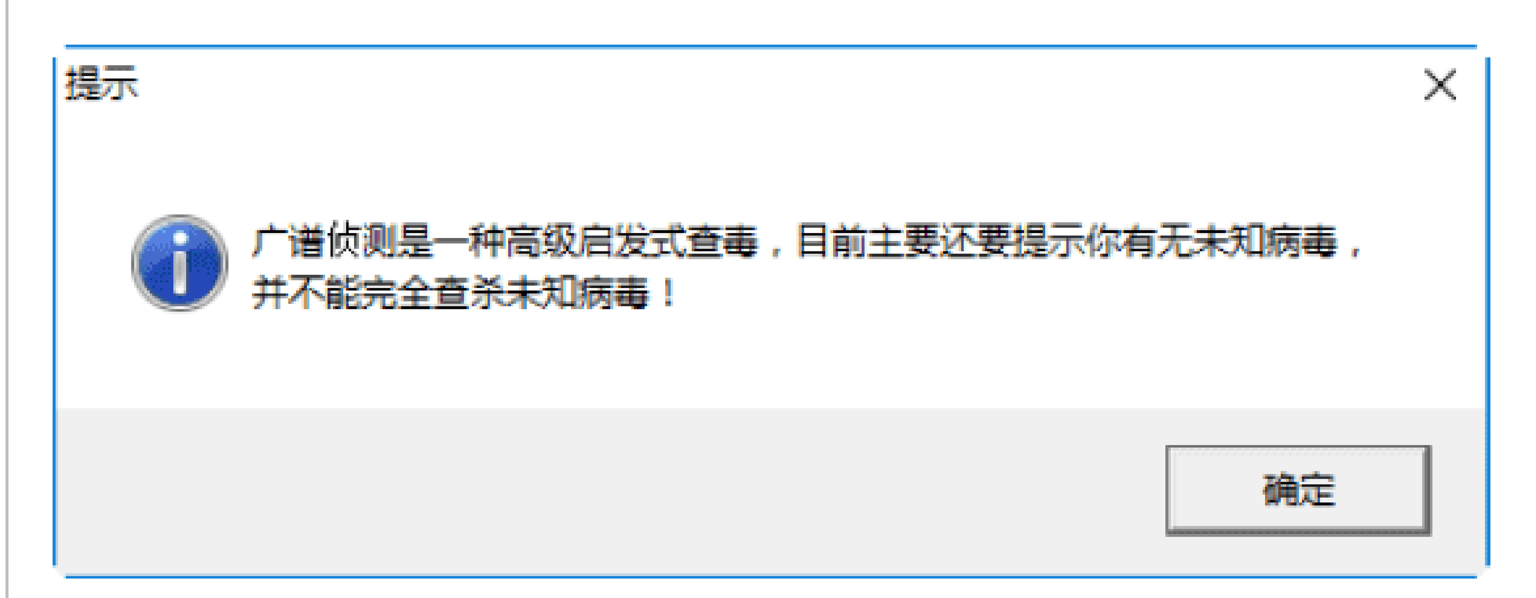


Step 09 待检测完毕后，会在“移动存储病毒处理模块V1.1”对话框中看到相应的操作日志，如下图所示。

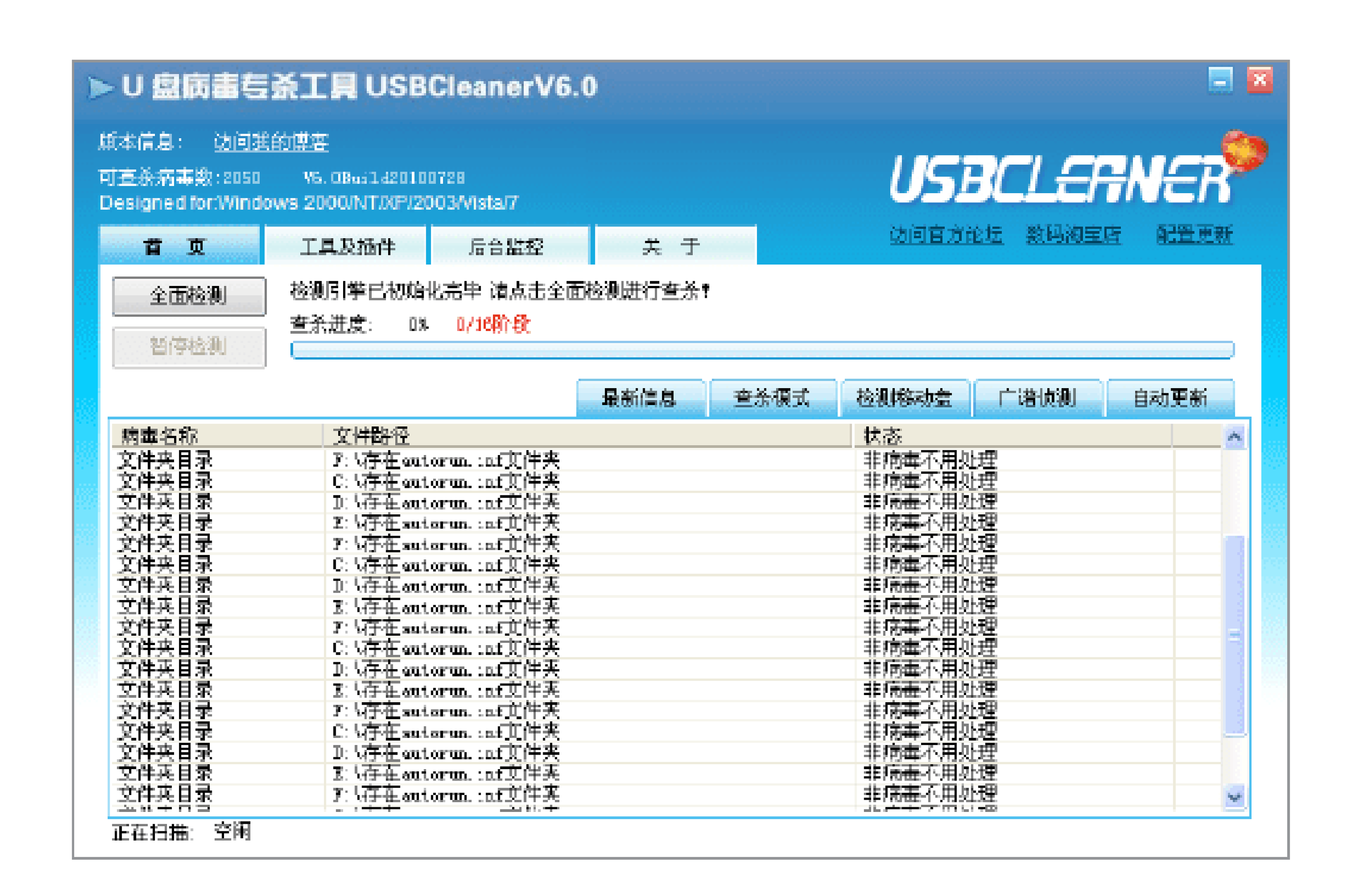


3. 检测未知病毒

Step 01 在“U盘病毒专杀工具USBCleaner V6.0”对话框中单击“广谱侦测”按钮，即可看到“不能完全查杀未知病毒”对话框，如下图所示。



Step 02 单击“确定”按钮，即可进行广谱侦测，待侦测完毕后，会把本机中的所有autorun.inf文件列出来，如下图所示。



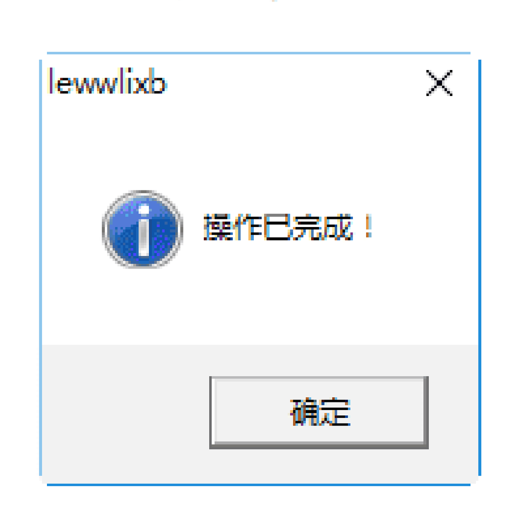
Step 03 在“U盘病毒专杀工具USBCleaner V6.0”对话框中选择“工具及插件”选项卡，在其中可以对U盘病毒免疫、移动盘卸载、USB设备痕迹清理、系统修复等属性进行设置，如下图所示。



Step 04 单击“USB设备痕迹清理”按钮，打开“USB设备使用记录清理”对话框，在其中显示了USB设置的使用记录，如下图所示。



Step 05 单击“清理所有记录”按钮，即可将所有的USB使用记录清除，如下图所示。



Step 06 选择“后台监控”选项卡，在桌面上的状态栏中双击“USBMON监控程式”图标，即可打开如下图所示的对话框，在其中可以对监控的各个属性进行设置。



Step 07 单击“其他功能”按钮，在打开的窗口中即可对U盘的写保护和文件目录强制删除进行设置，如下图所示。



4.6　实战演练

实战演练1——在Word中预防宏病毒

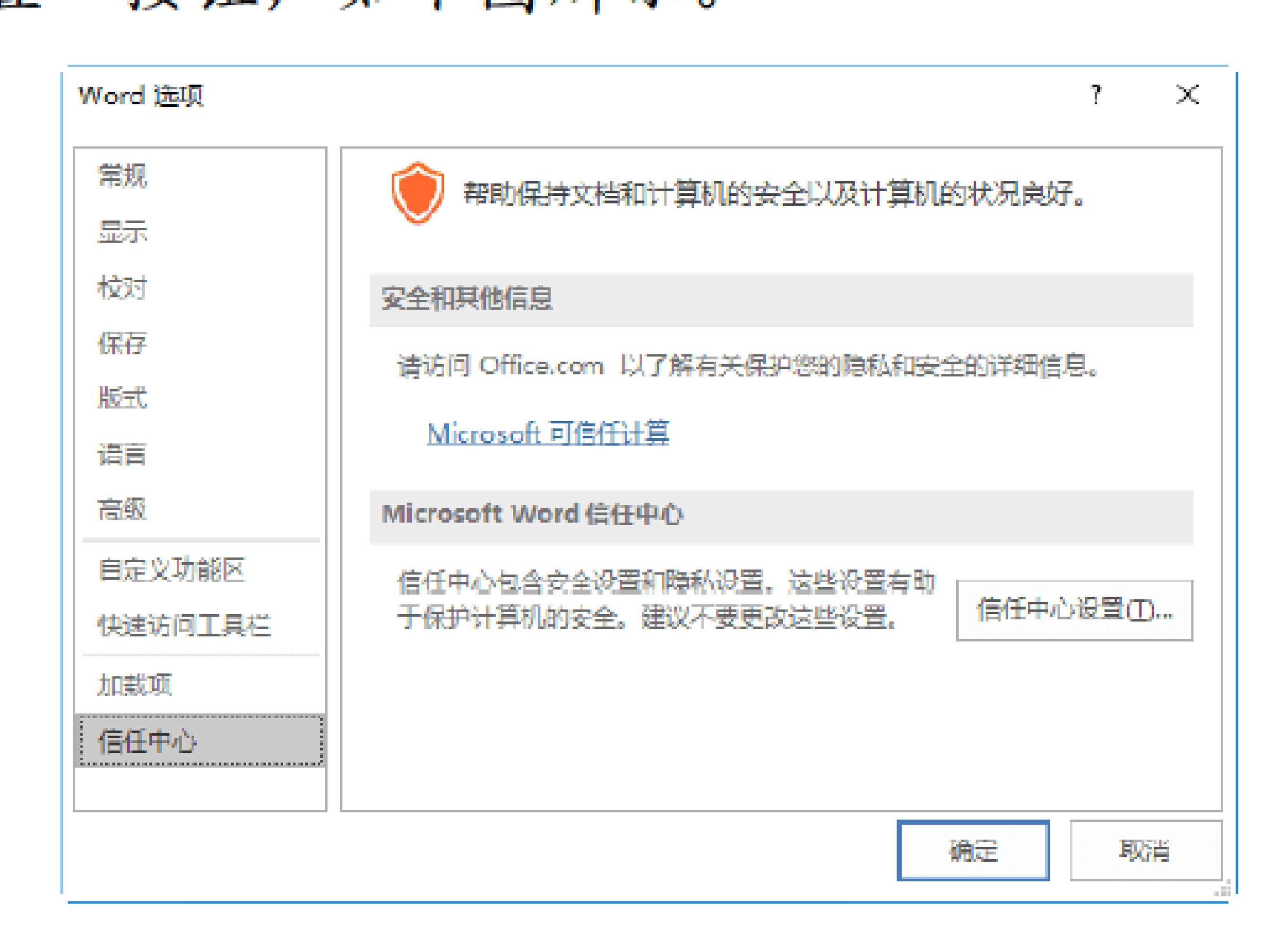


包含宏的工作簿更容易感染病毒，所以用户需要提高宏的安全性。下面以在Word 2016中预防宏病毒为例，介绍预防宏病毒的方法，具体操作步骤如下。

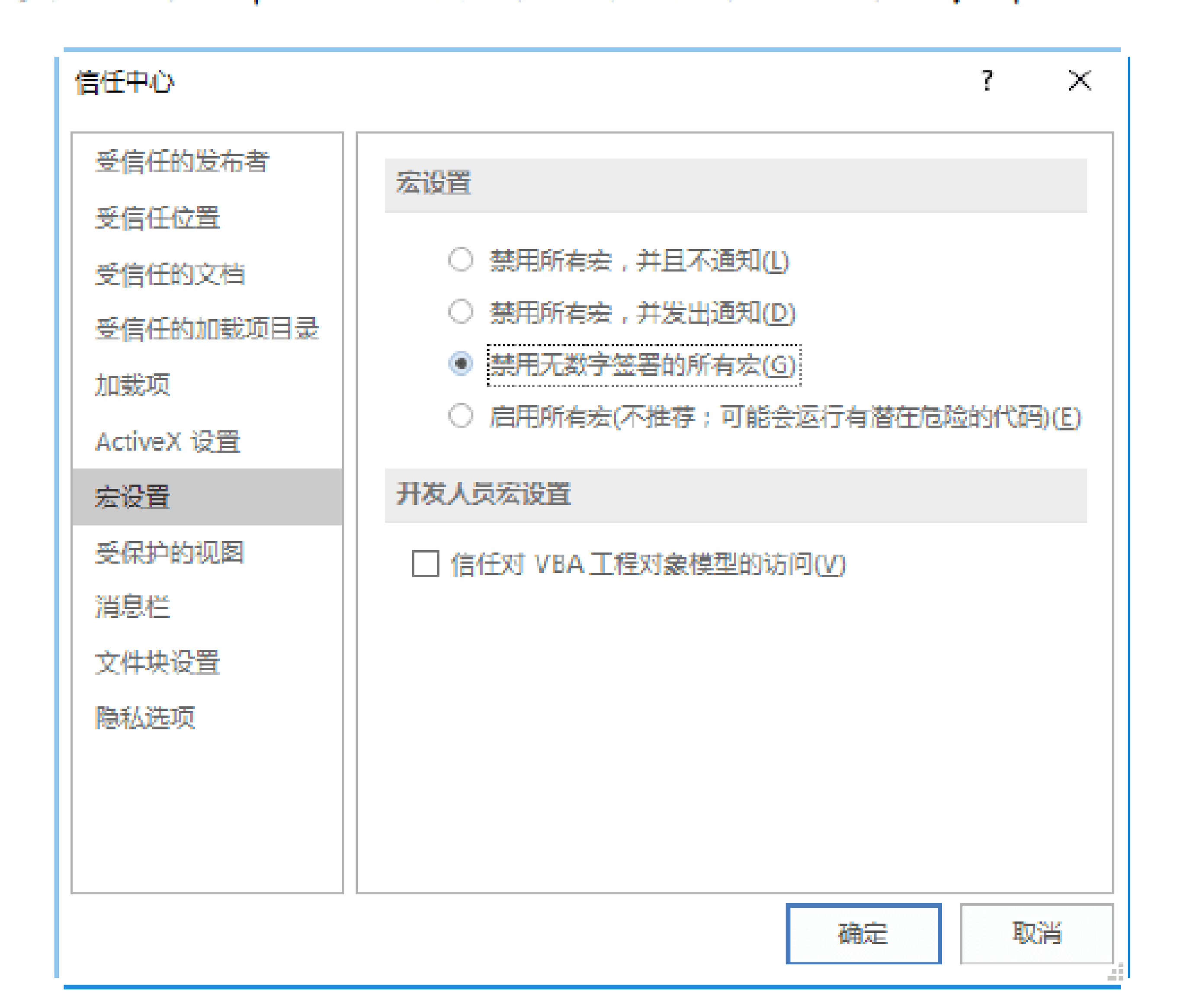
Step 01 打开包含宏的工作簿，选择“文件”→“选项”选项，如下图所示。



Step 02 打开“Word选项”对话框，选择“信任中心”选项，然后单击“信任中心设置”按钮，如下图所示。



Step 03 弹出“信任中心”对话框，在左侧列表中选择“宏设置”选项，然后在“宏设置”列表中选中“禁用无数字签署的所有宏”单选按钮，单击“确定”按钮，如下图所示。







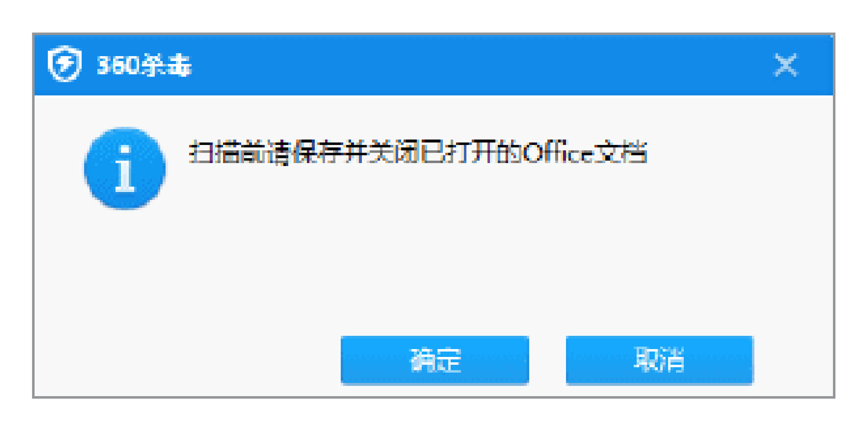
实战演练2——使用《360杀毒》查杀宏病毒

使用《360杀毒》还可以对Office宏病毒进行查杀。具体的操作步骤如下。

Step 01 在360杀毒的主界面中单击“宏病毒扫描”图标，如下图所示。



Step 02 弹出“360杀毒”对话框，提示用户扫描前需要关闭已经打开的Office文档，如下图所示。



Step 03 单击“确定”按钮，即可开始扫描计算机中的宏病毒，并显示扫描的进度，如下图所示。



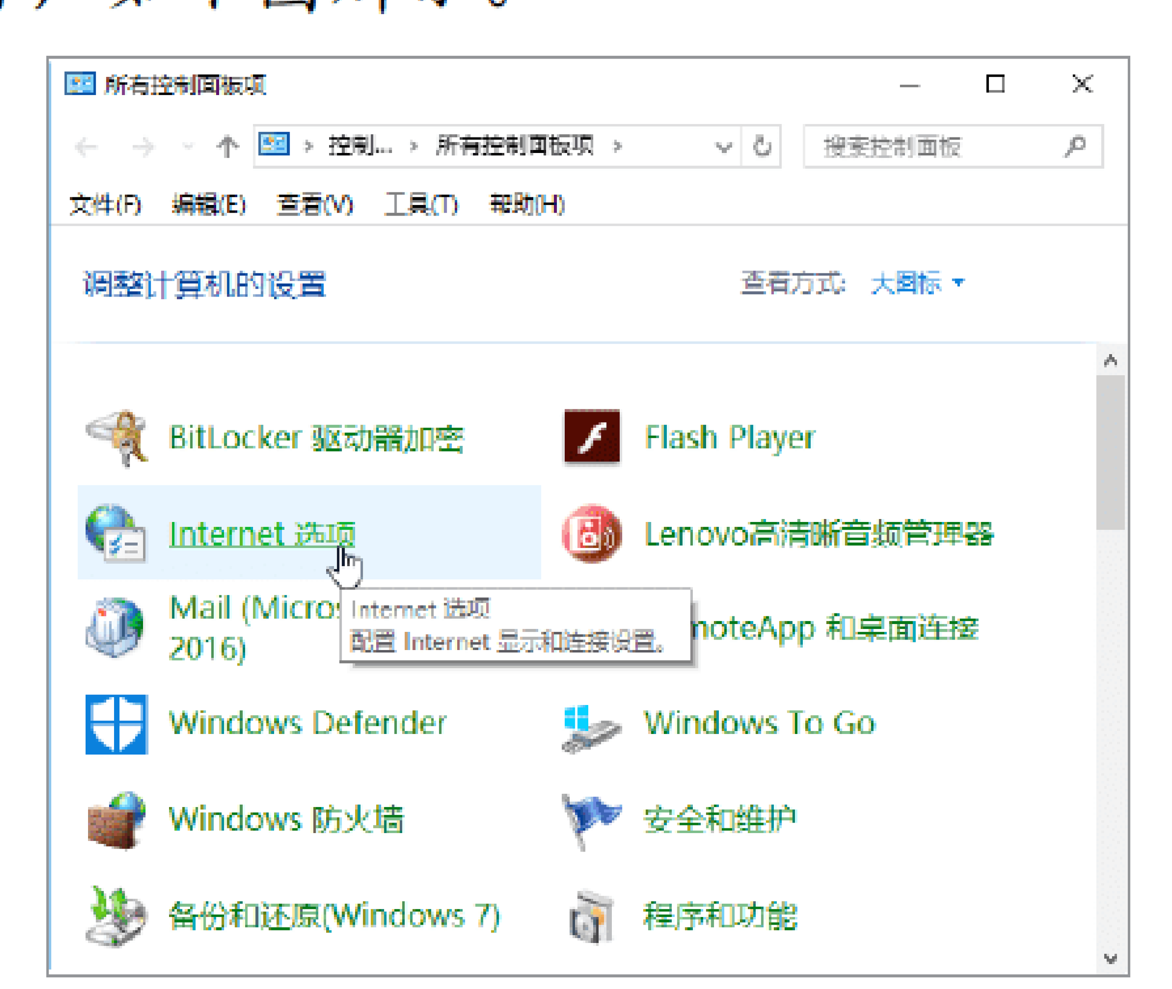
Step 04 扫描完成后，即可对扫描出来的宏病毒进行处理。这与“快速查杀”相似，这里不再详细介绍。

4.7 小试身手

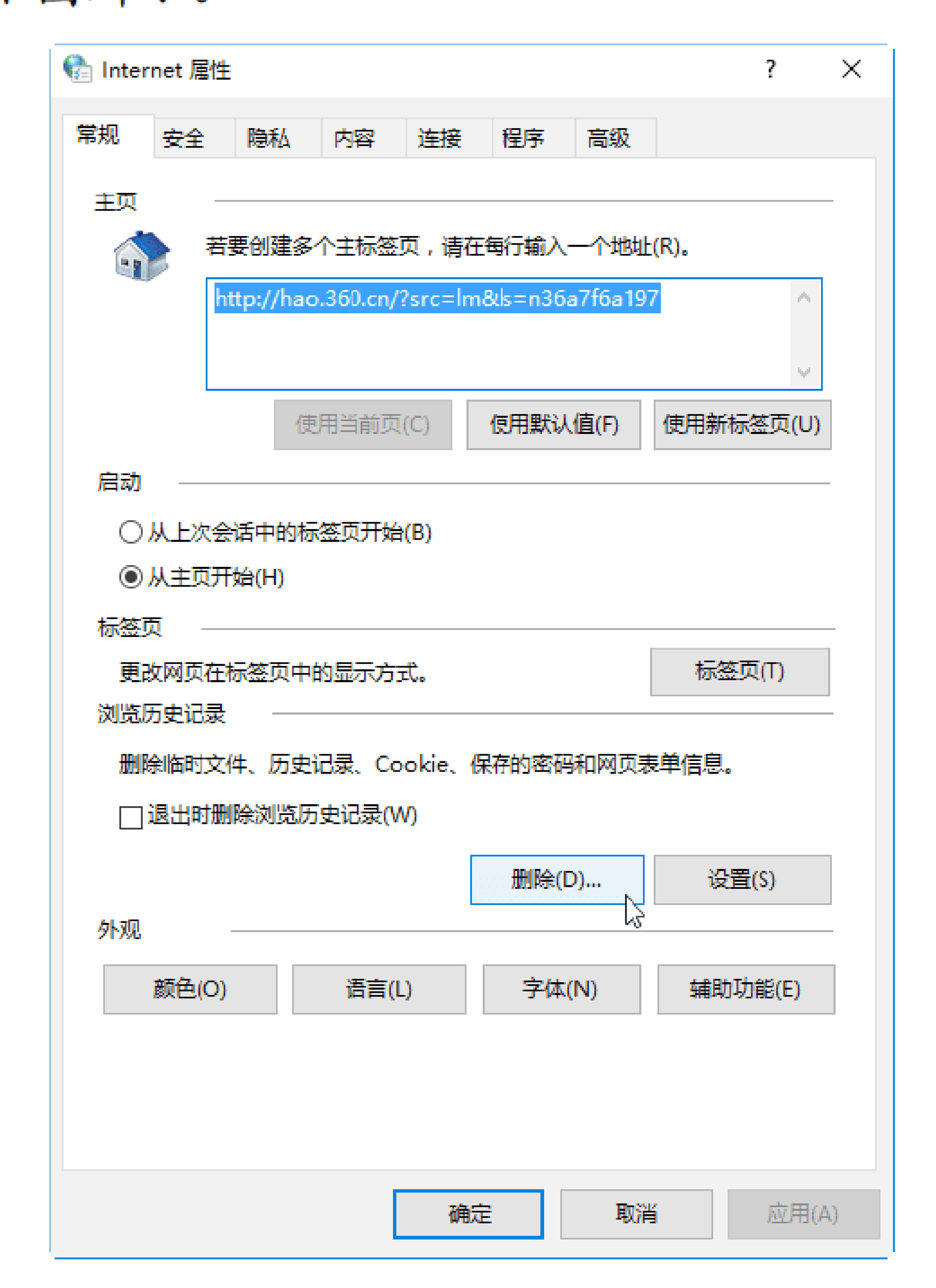
练习1：删除上网缓存文件

用户可以通过“Internet选项”对话框删除平时上网的缓存文件。具体操作步骤如下。

Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”选项，打开“所有控制面板项”窗口，单击“Internet选项”图标，如下图所示。



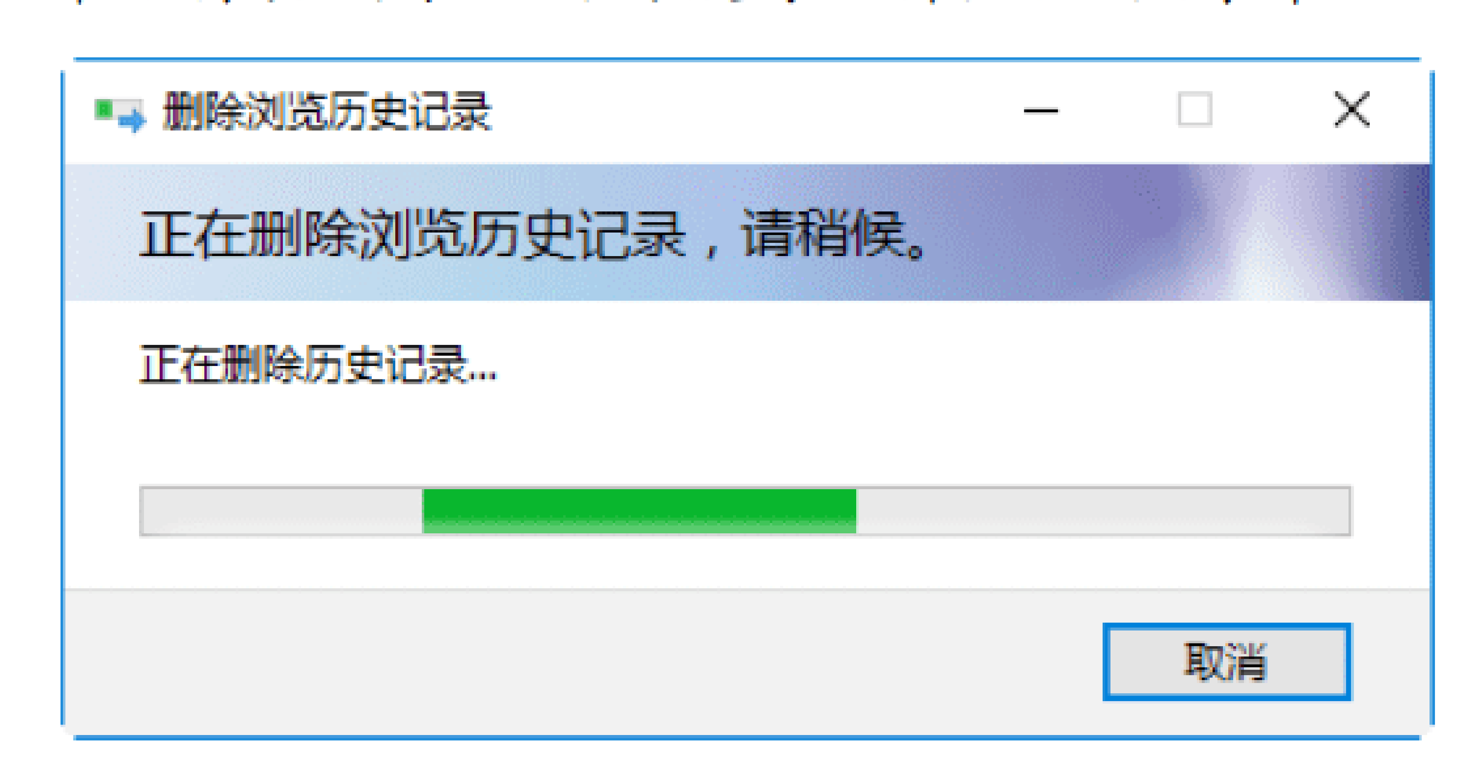
Step 02 弹出“Internet属性”对话框，单击“浏览历史记录”下的“删除”按钮，如下图所示。



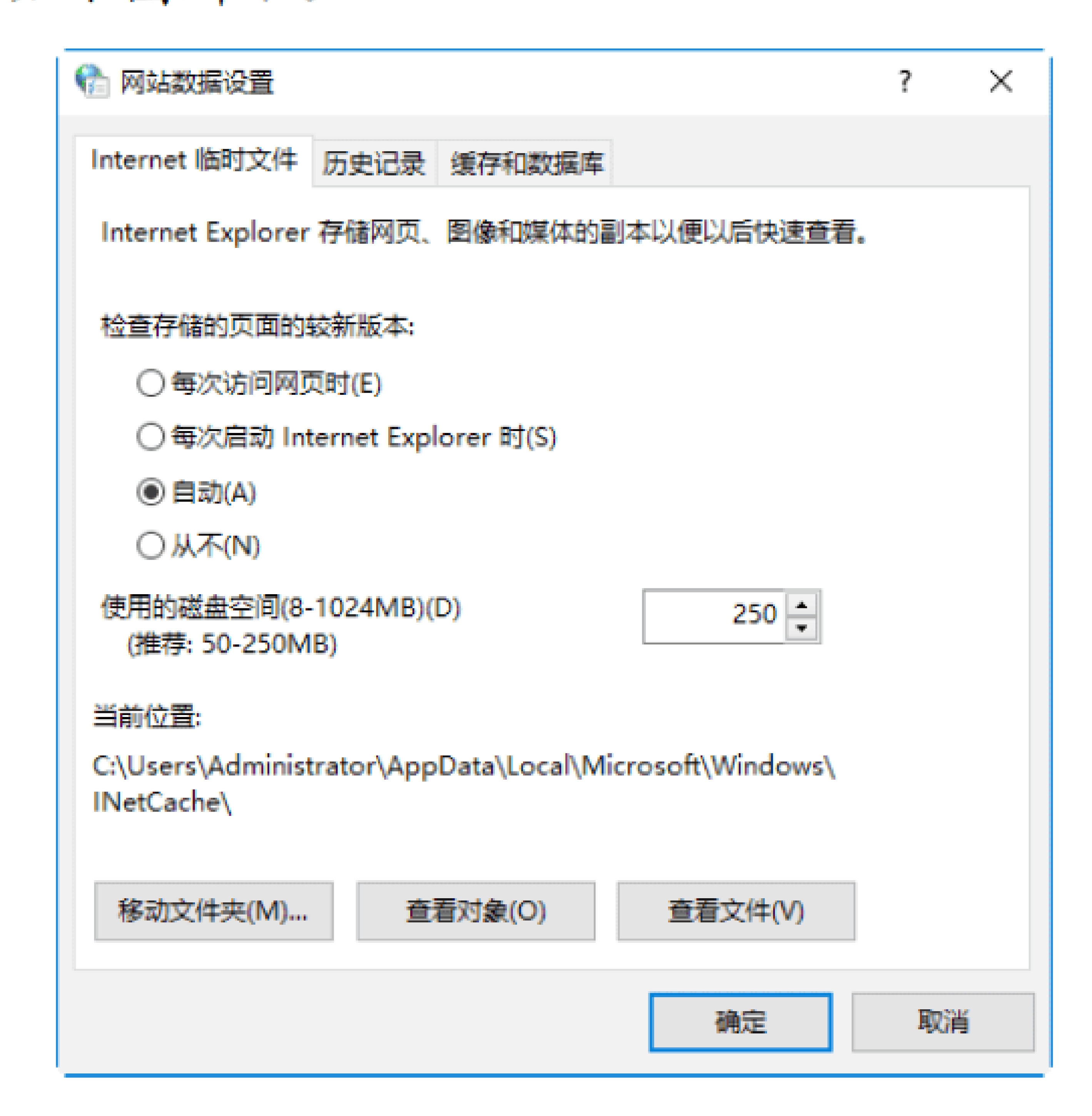
Step 03 弹出“删除浏览历史记录”对话框，选择需要删除的缓存文件类型，单击“删除”按钮，如下图所示。



Step 04 弹出“删除浏览历史记录”窗口，系统开始自动删除上网的缓存文件，如下图所示。



Step 05 删除完成后，返回到“Internet属性”对话框，单击“浏览历史记录”下的“设置”按钮。弹出“网站数据设置”对话框，设置缓存的大小和保存天数，单击“移动文件夹”按钮，可以转移缓存文件的位置，单击“确定”按钮，完成设置，如下图所示。



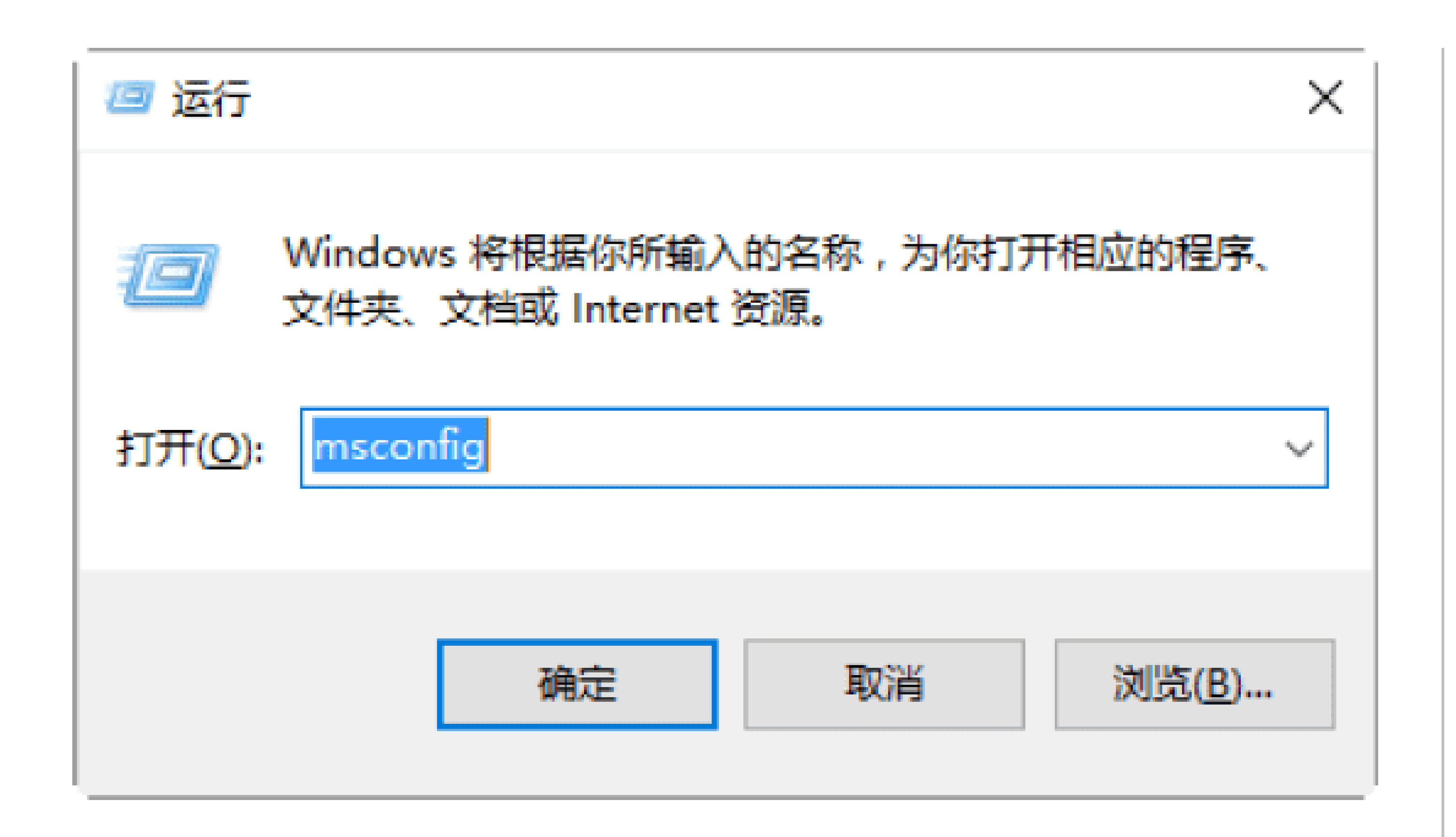
练习2：在安全模式下查杀病毒



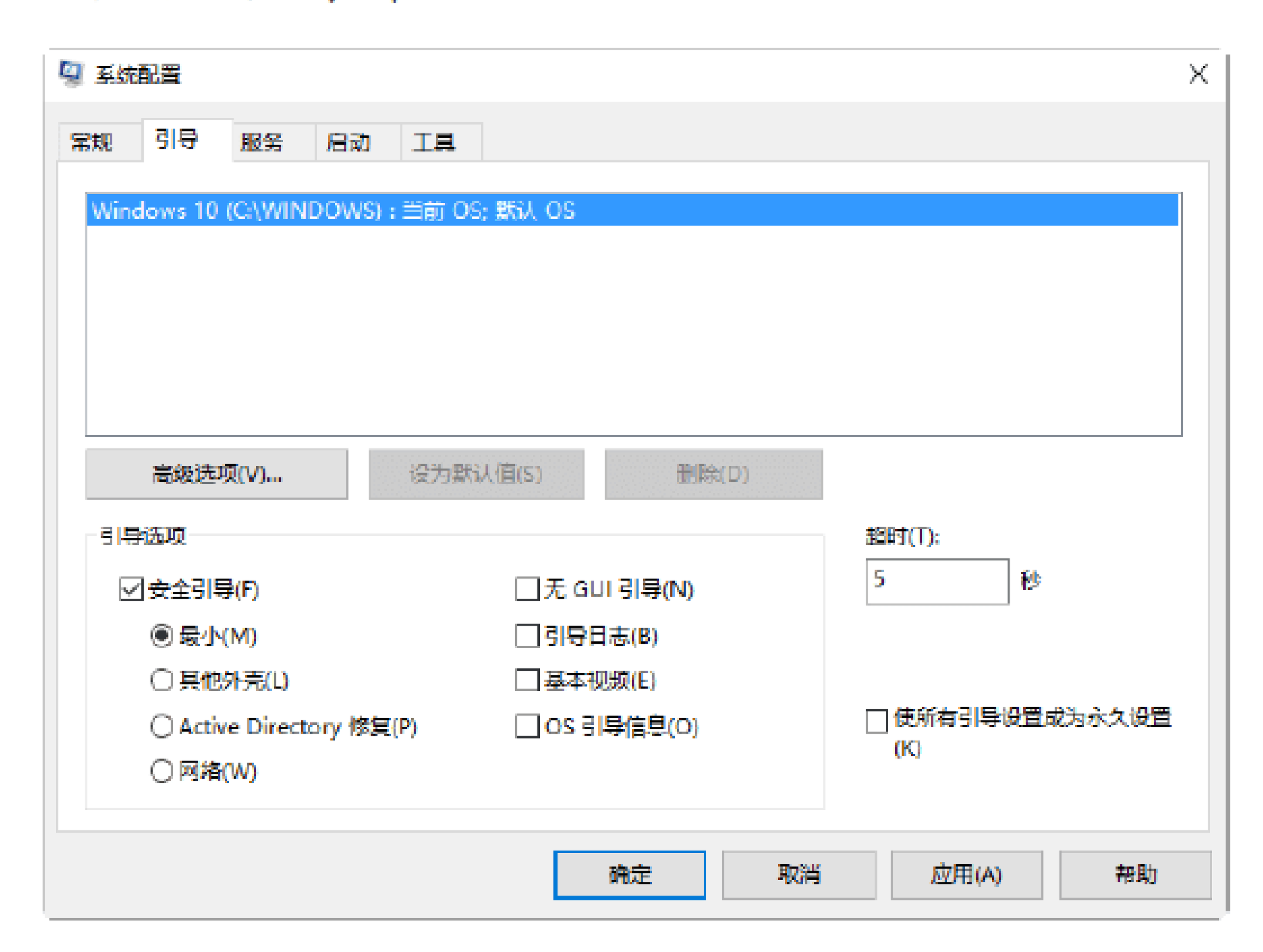
安全模式的工作原理是在不加载第三方设备驱动程序的情况下启动计算机，使计算机运行在系统最小模式，这样用户就可以方便地查杀病毒，还可以检测与修复计算机系统的错误。下面以Windows 10操作系统为例，介绍在安全模式下查杀病毒的方法。

具体的操作步骤如下。

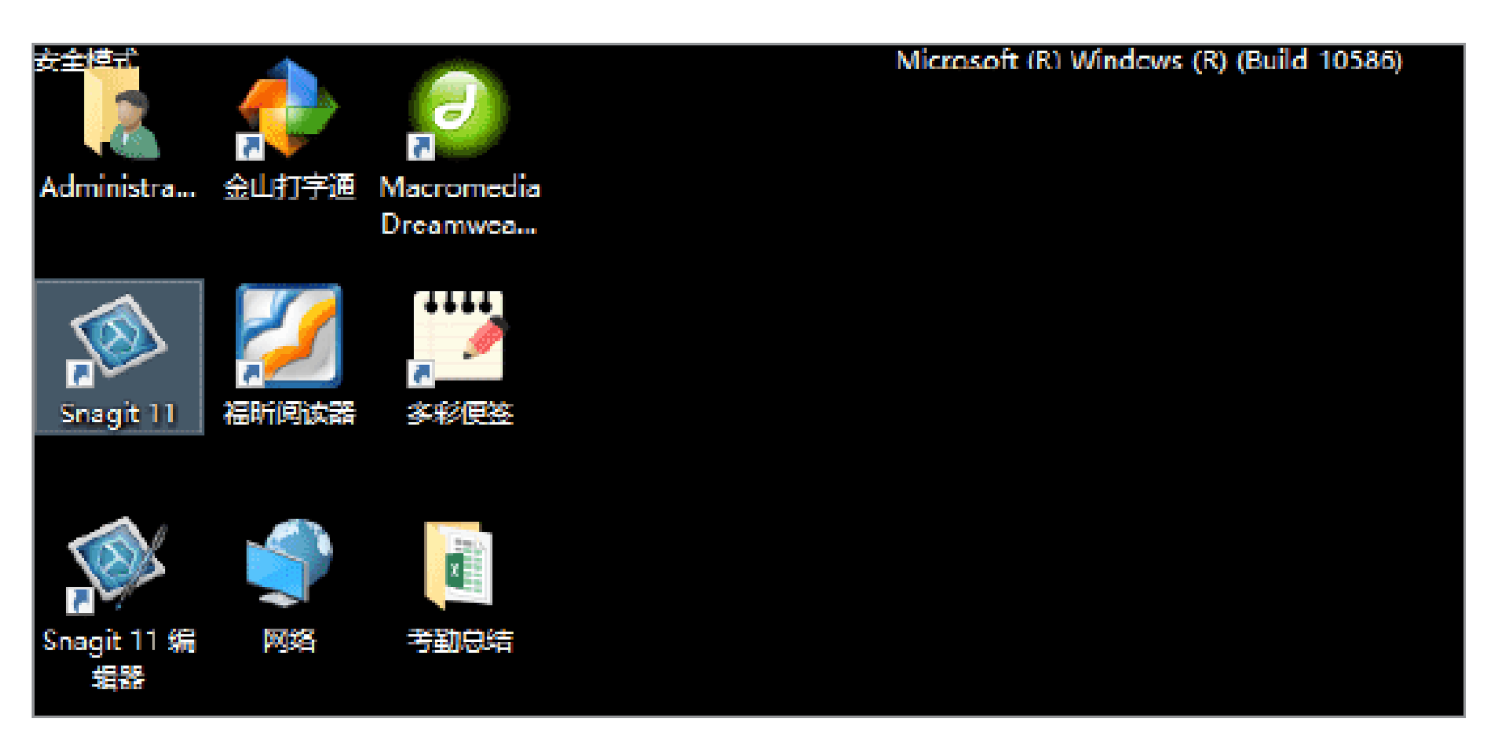
Step 01 按WIN+R组合键，弹出“运行”对话框，在“打开”文本框中输入msconfig命令，单击“确定”按钮，如下图所示。



Step 02 弹出“系统配置”对话框，选择“引导”选项卡，在“引导选项”中勾选“安全引导”复选框和选中“最小”单选按钮，如下图所示。



Step 03 单击“确定”按钮，即可进入系统的安全模式，如下图所示。



Step 04 进入安全模式后，即可运行杀毒软件，进行病毒的查杀，如下图所示。



第5章　系统漏洞与用户账户的安全防护

当前，用户普遍使用的操作系统为Windows 10，不过，该系统也存在这样或那样的安全问题，如系统漏洞、系统账户等，这就给黑客留下了入侵攻击的机会。本章介绍系统漏洞与用户账户的安全防护，主要内容包括系统漏洞的安全防护、系统账户的安全防护等。

5.1　认识系统漏洞与用户账户

计算机系统漏洞也被称为系统安全缺陷，这些安全缺陷常常被黑客所利用，从而达到其控制目标主机或造成一些更具破坏性的影响的目的。用户账户相当于进入计算机的“守门员”，一旦为这个“守门员”设置了密码，这在一定程度上会提升计算机系统的安全性。

5.1.1　认识计算机系统漏洞

漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误，某个程序（包括操作系统）在设计时未考虑周全，则这个缺陷或错误将可能被不法分子或黑客利用，通过植入木马、病毒等方式来攻击或控制整个计算机，从而窃取计算机中的重要资料和信息，甚至破坏系统。

系统漏洞又称安全缺陷，可对用户造成不良后果。若漏洞被恶意用户利用，会造成信息泄漏；黑客攻击网站即利用网络服务器操作系统的漏洞，对用户操作造成不便，如不明原因的死机和丢失文件等。

5.1.2　系统漏洞产生的原因

系统漏洞的产生不是安装不当的结果，也不是使用后的结果，归结起来，其产生的原因主要有以下几点。

（1）人为因素：编程人员在编写程序过程中故意在程序代码的隐蔽位置保留了后门。

（2）硬件因素：因为硬件的原因，编程人员无法弥补硬件的漏洞，从而使硬件问题通过软件表现出来。

（3）客观因素：受编程人员的能力、经验和当时的安全技术及加密方法发展水平所限，在程序中难免存在不足之处，而这些不足恰恰会导致系统漏洞的产生。

5.1.3　认识本地管理员账户

在Windows 7及其之前的操作系统中，Windows的安装和登录只有一种以用户名为标识符的账户，这个账户就是Administrator账户，这种账户类型就是本地账户。对于不需要网络功能，而又对数据安全比较在乎的用户来说，使用本地账户登录Windows 10操作系统是更安全的选择。

另外，对于本地账户来说，用户可以不用设置登录密码，就能登录系统。当然，不设置密码的操作，对系统安全是没有保障的。因此，不管是本地账户，还是Microsoft账户，都需要为账户添加密码。

5.1.4　认识Microsoft账户

Microsoft账户是免费的且易于设置的

系统账户，用户可以使用自己所选的任何电子邮件地址完成该账户的注册与登记操作。例如，可以使用Outlook.com、Gmail或Yahoo!地址作为Microsoft账户。

当用户使用Microsoft账户登录自己的计算机或设备时，可从Windows应用商店中获取应用，使用免费云存储备份自己的所有重要数据和文件，并使自己的所有常用内容（如设备、照片、好友、游戏、个人偏好设置、音乐等）保持更新和同步。

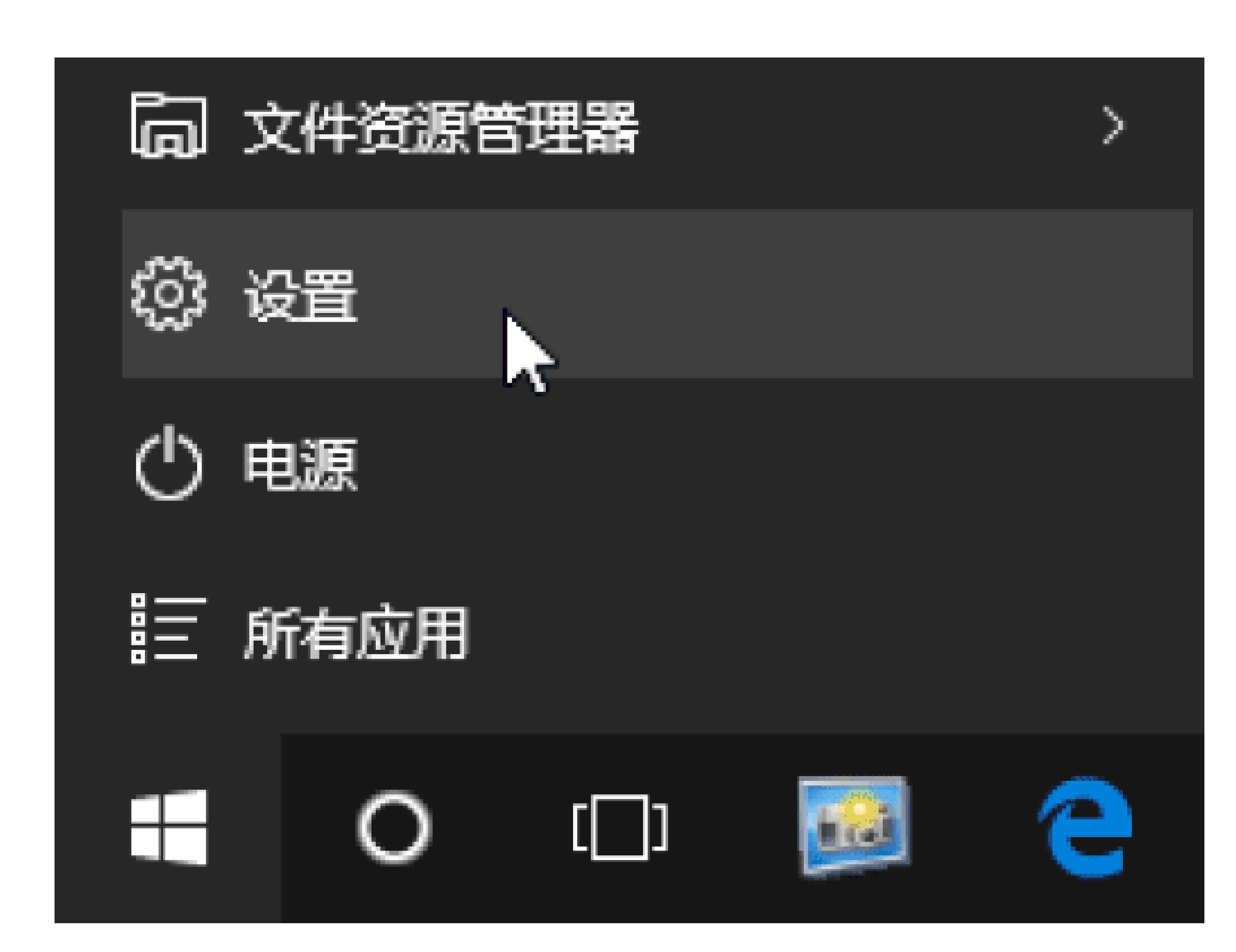
5.2　系统漏洞的安全防护

要想防范系统的漏洞，首选就是及时为系统打补丁。修复系统漏洞的常用方法有两种：一种是使用Windows更新修复系统漏洞；一种是使用360安全卫士修复系统漏洞。

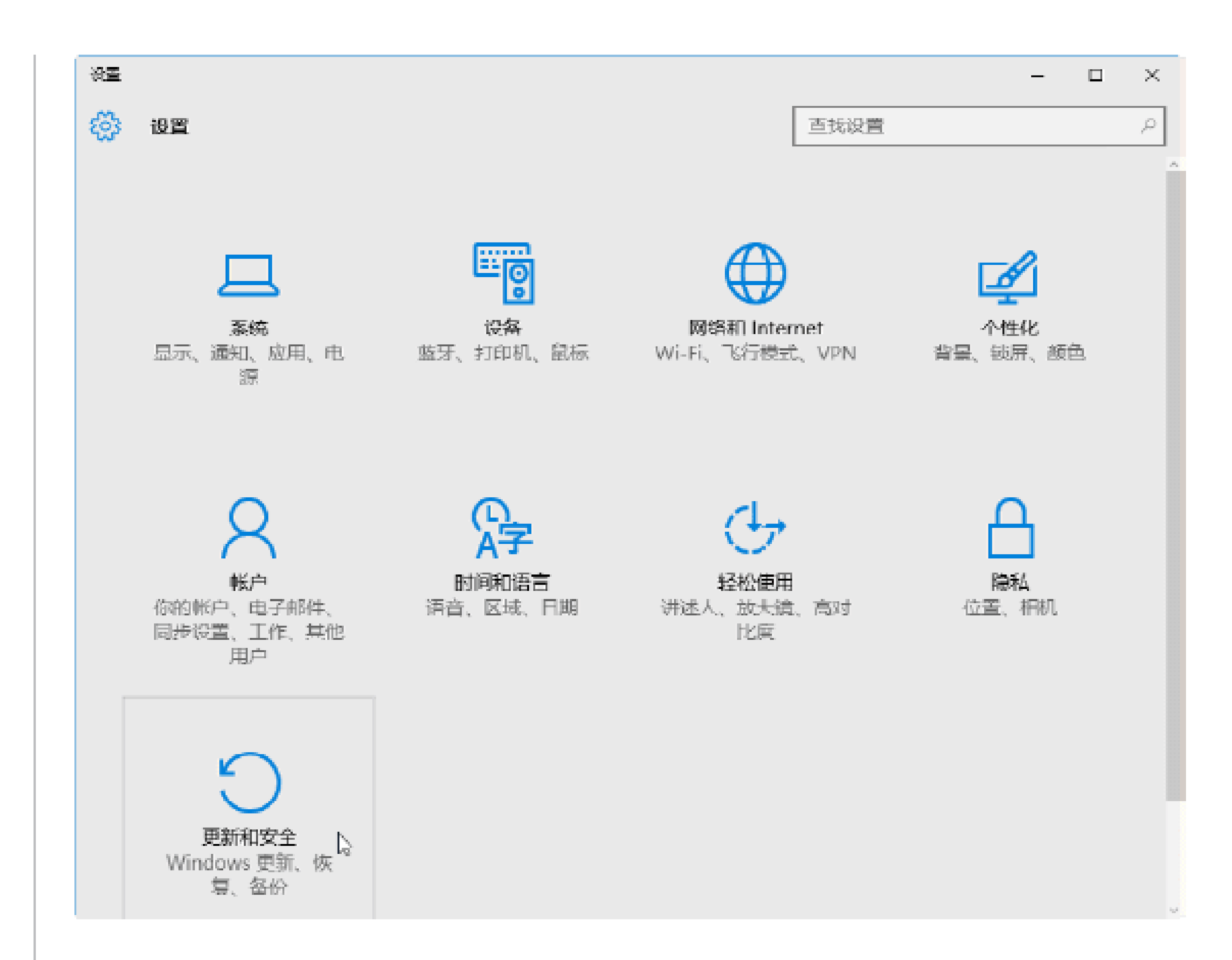
实战1：使用“Windows更新”修复系统漏洞

“Windows更新”是系统自带的用于检测系统更新的工具，使用“Windows更新”可以下载并安装系统更新。以Windows 10系统为例，具体的操作步骤如下。

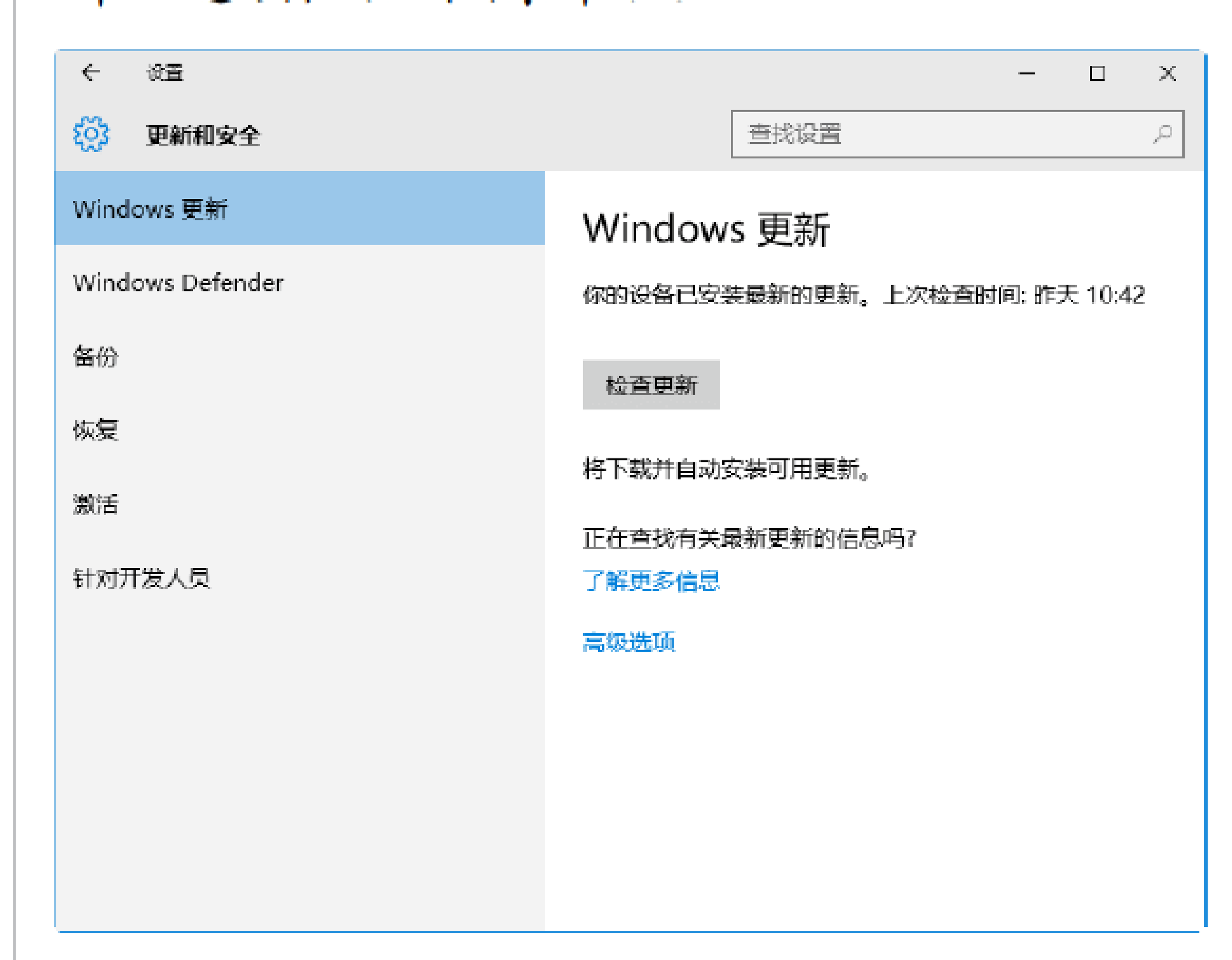
Step 01 单击“开始”按钮，在打开的菜单中选择“设置”选项，如下图所示。



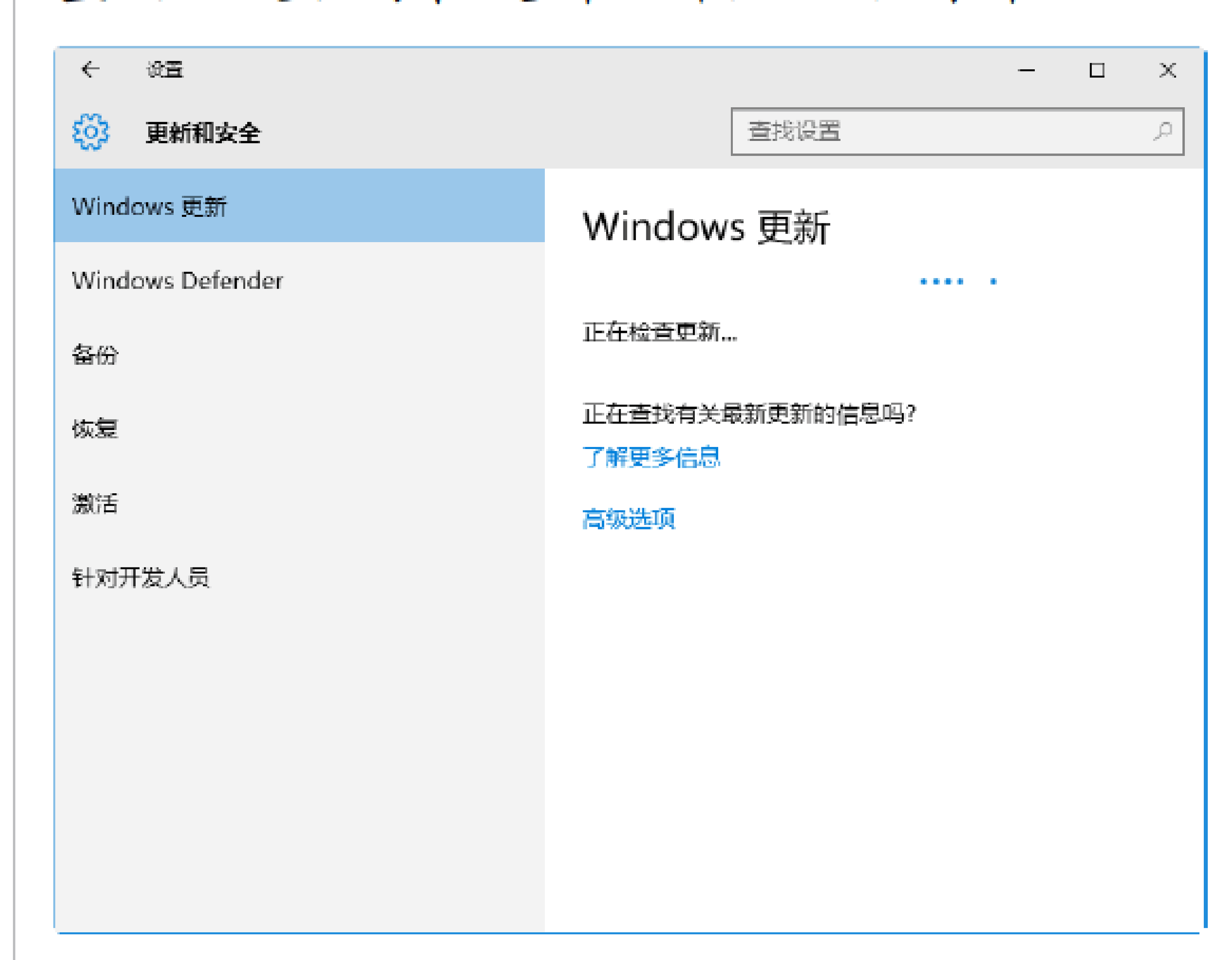
Step 02 打开“设置”窗口，在其中可以看到有关系统设置的相关功能，如下图所示。



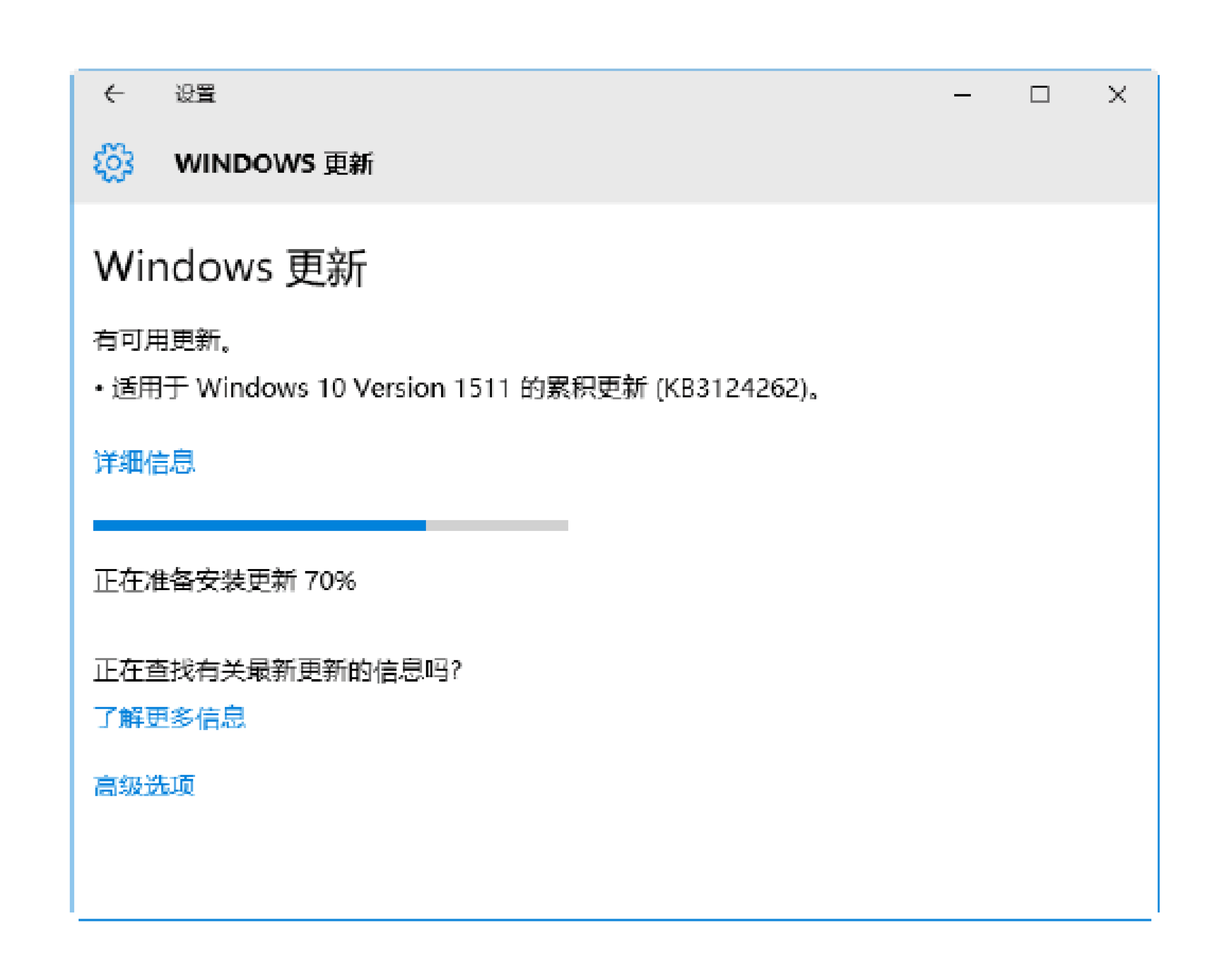
Step 03 单击“更新和安全”图标，打开“更新和安全”窗口，在其中选择“Windows更新”选项，如下图所示。



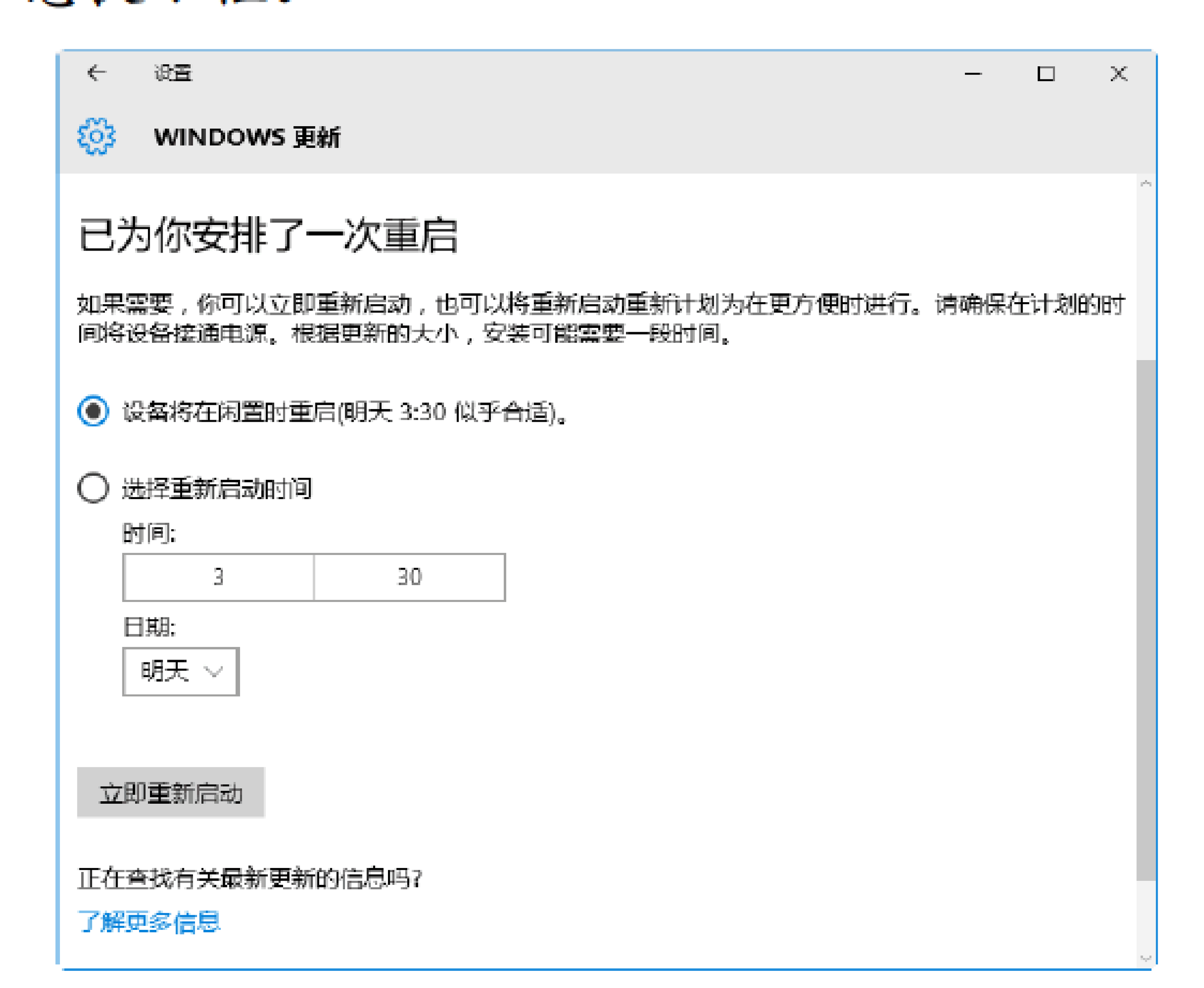
Step 04 单击“检查更新”按钮，即可开始检查网上是否存在更新文件，如下图所示。



Step 05 检查完毕后，如果存在更新文件，则会弹出如下图所示的信息提示，提示用户有可用更新，并自动下载更新文件。



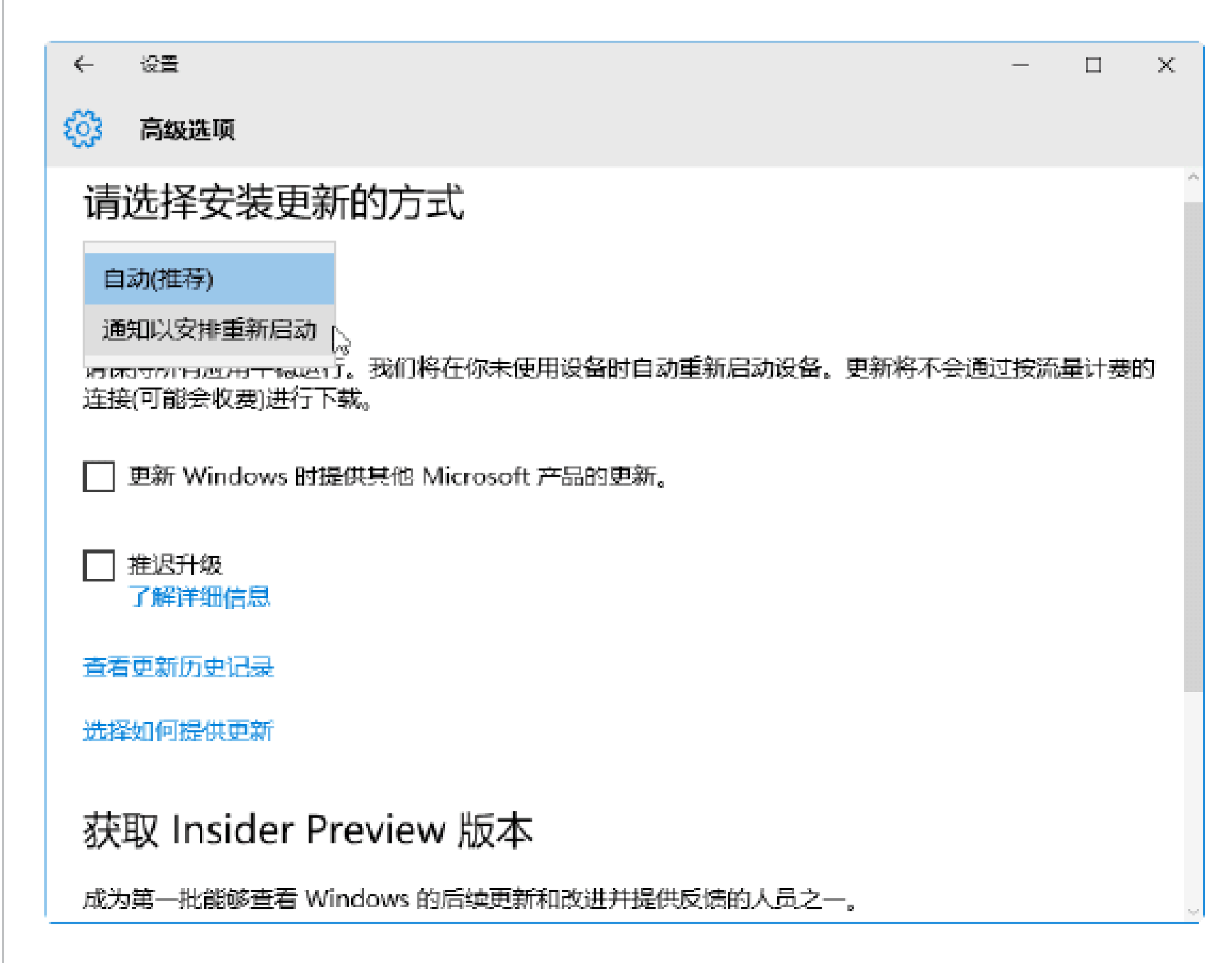
Step 06 下载完成后，系统会自动安装更新文件，安装完毕后，会弹出如下图所示的信息提示框。



Step 07 单击“立即重新启动”按钮，则会立即重新启动计算机。重新启动完毕后，再次打开“Windows更新”窗口，在其中可以看到“你的设备已安装最新的更新”信息提示，如下图所示。



Step 08 单击“高级选项”超链接，打开“高级选项”设置工作界面，在其中可以选择安装更新的方式，如下图所示。



实战2：使用《360安全卫士》修复系统漏洞

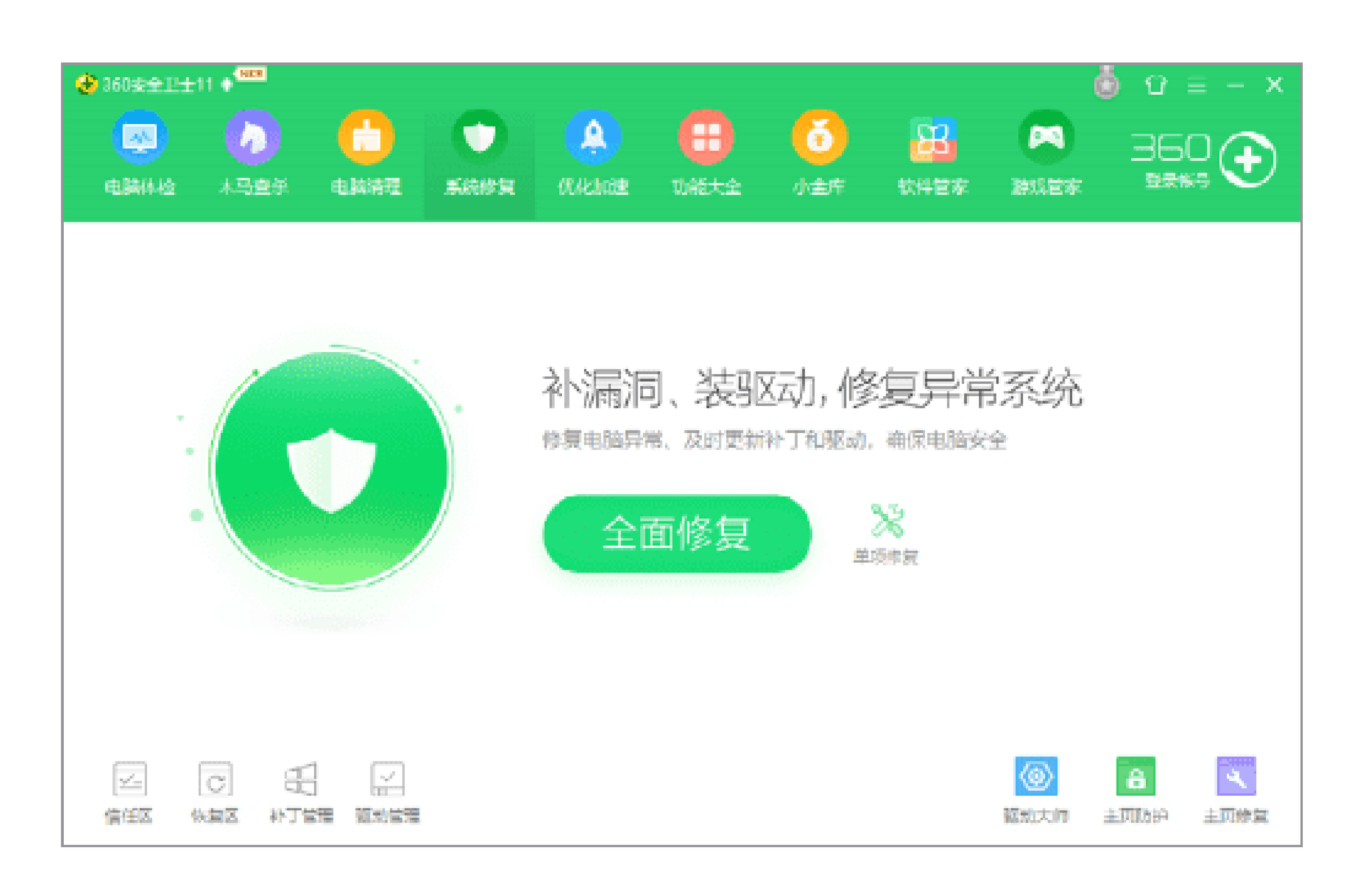
除使用Windows系统自带的“Windows更新”及时为系统更新修复漏洞外，还可以使用第三方软件及时为系统下载并安装漏洞补丁，常用的有《360安全卫士》《优化大师》等。

使用《360安全卫士》修复系统漏洞的具体操作步骤如下。

Step 01 双击桌面360安全卫士图标，打开“360安全卫士”窗口，如下图所示。



Step 02 单击“系统修复”按钮，进入如下图所示页面。



Step 03 单击“全面修复”按钮，360安全卫士开始自动扫描系统中存在的漏洞，并在下图所示的界面中显示出来，用户在其中可以自主选择需要修复的漏洞。



Step 04 单击“一键修复”按钮，开始修复系统存在的漏洞，如下图所示。



Step 05 修复完成后，则系统漏洞的状态变为“已修复”，如下图所示。



5.3　本地系统账户的安全防护

对本地系统账户的安全防护是保护系统安全的一种方式，主要内容包括启用本地账户，设置账户密码，删除用户账户等。

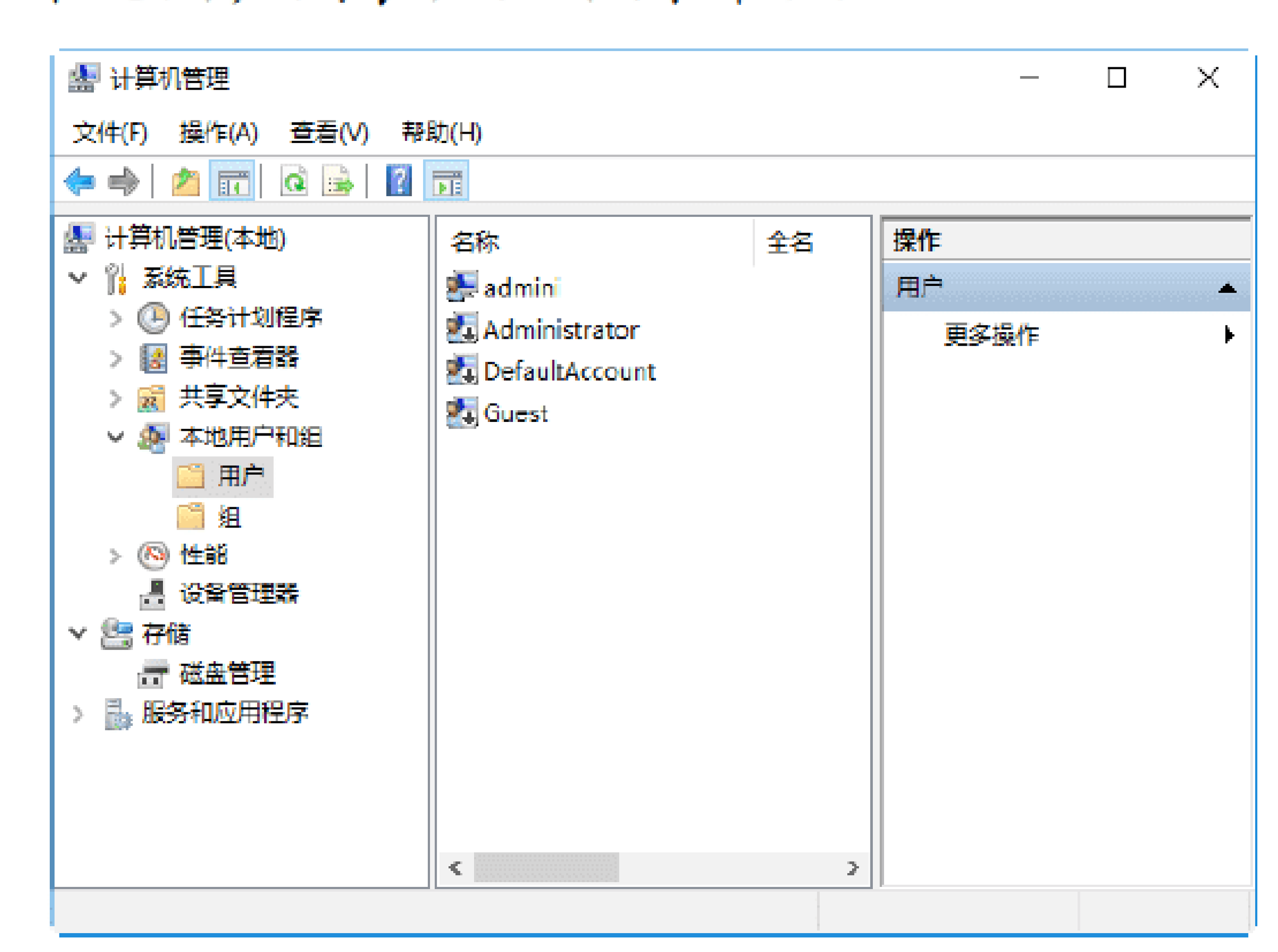
实战3：启用本地Administrator账户

在安装Windows 10系统的过程中，需要通过用户在微软注册的账户来激活系统，所以当安装完成以后，系统会默认用微软的账户来作为系统登录用户。不过，用户可以启用本地账户，这里以启用Administrator账户为例。启用Administrator账户的操作步骤如下。

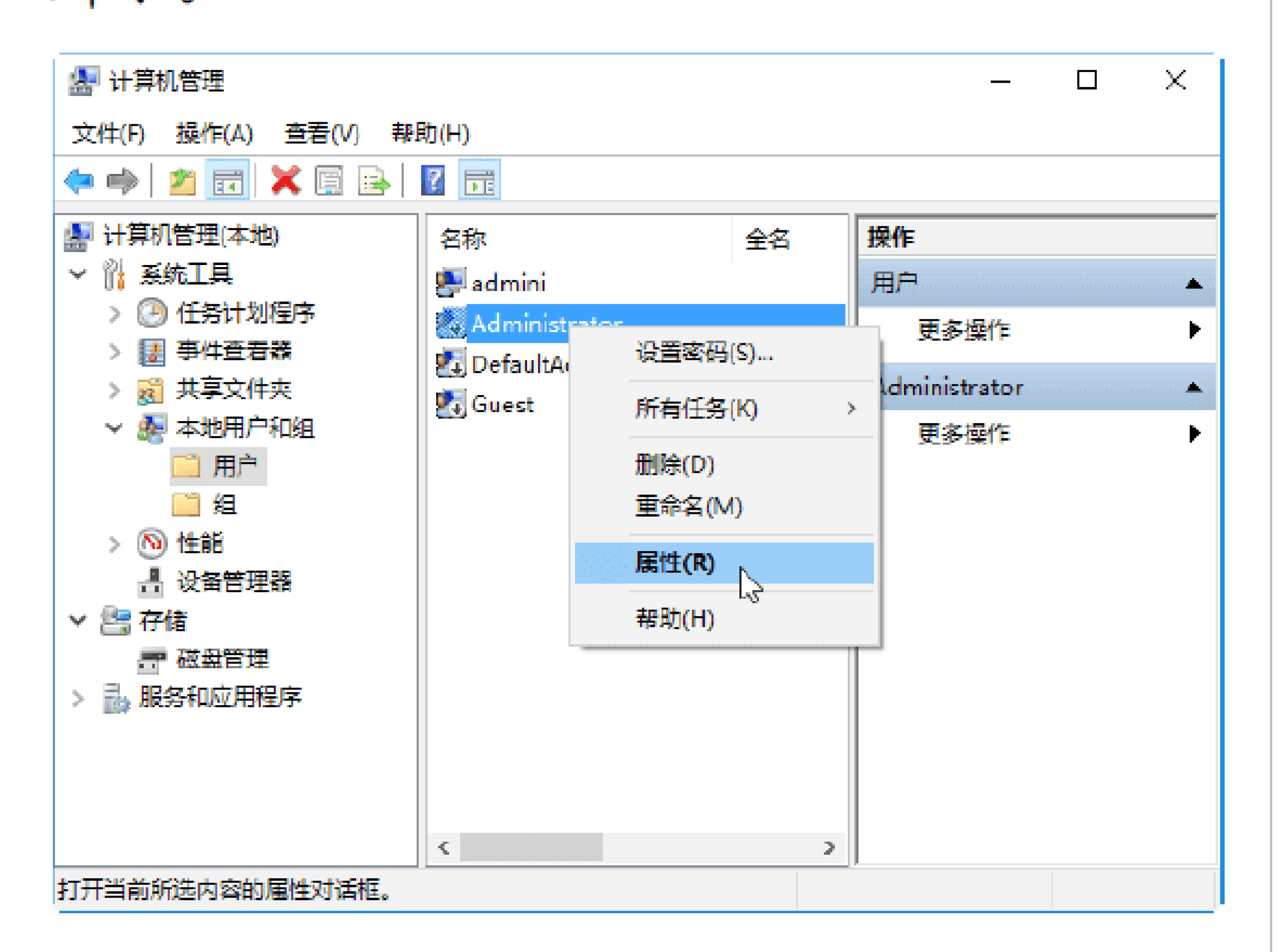
Step 01 在Windows 10系统桌面中，右击“开始”按钮，在弹出的快捷菜单中选择“计算机管理”选项，如下图所示。



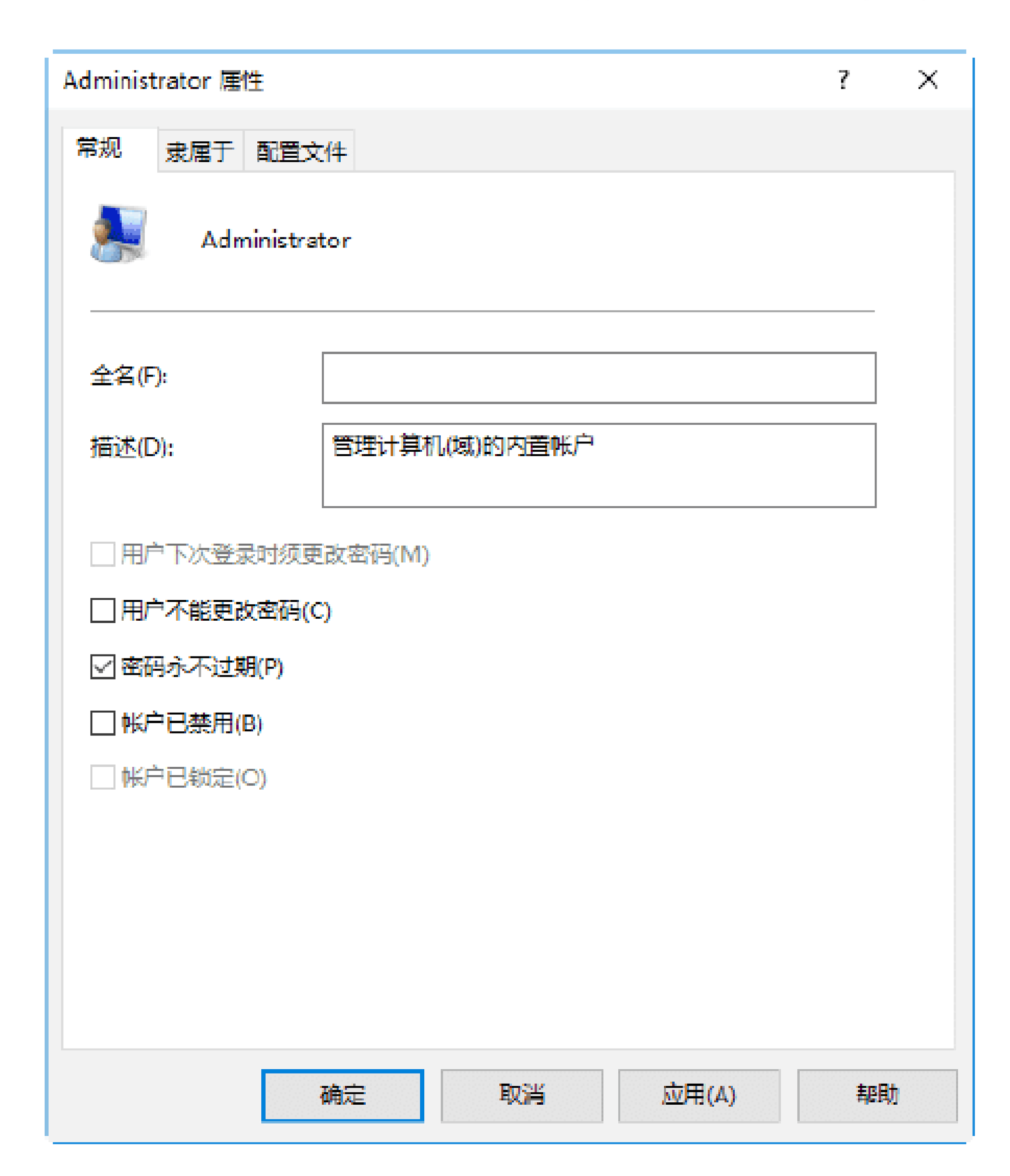
Step 02 打开“计算机管理”窗口，依次展开“本地用户和组”→“用户”选项，展开本地用户列表，如下图所示。



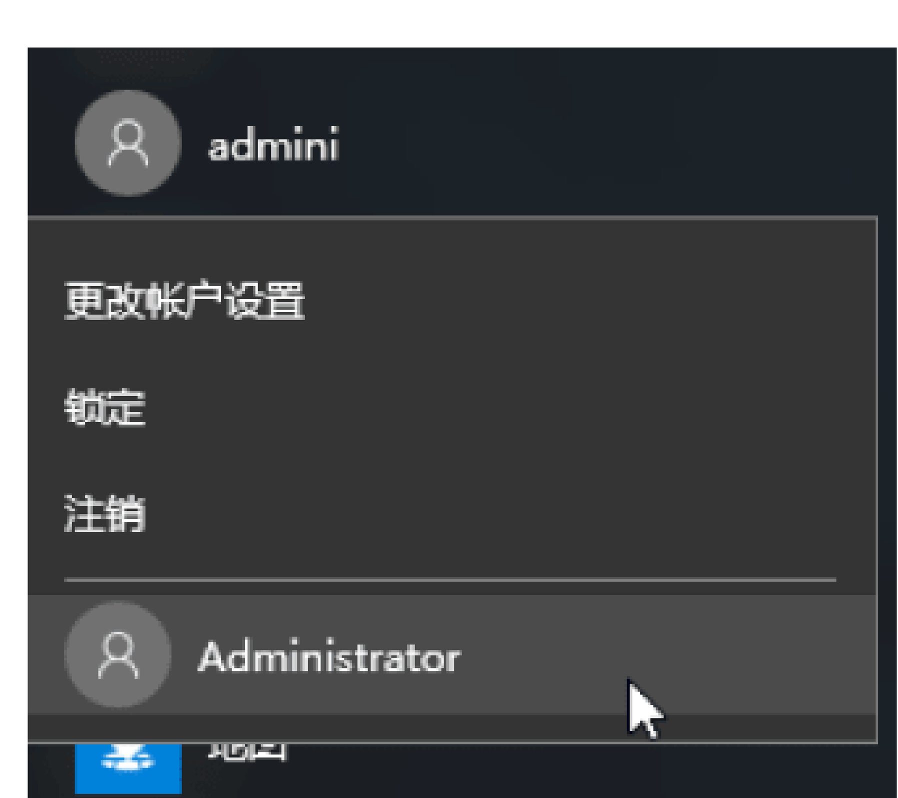
Step 03 右击Administrator账户，在弹出的快捷菜单中选择“属性”选项，如下图所示。



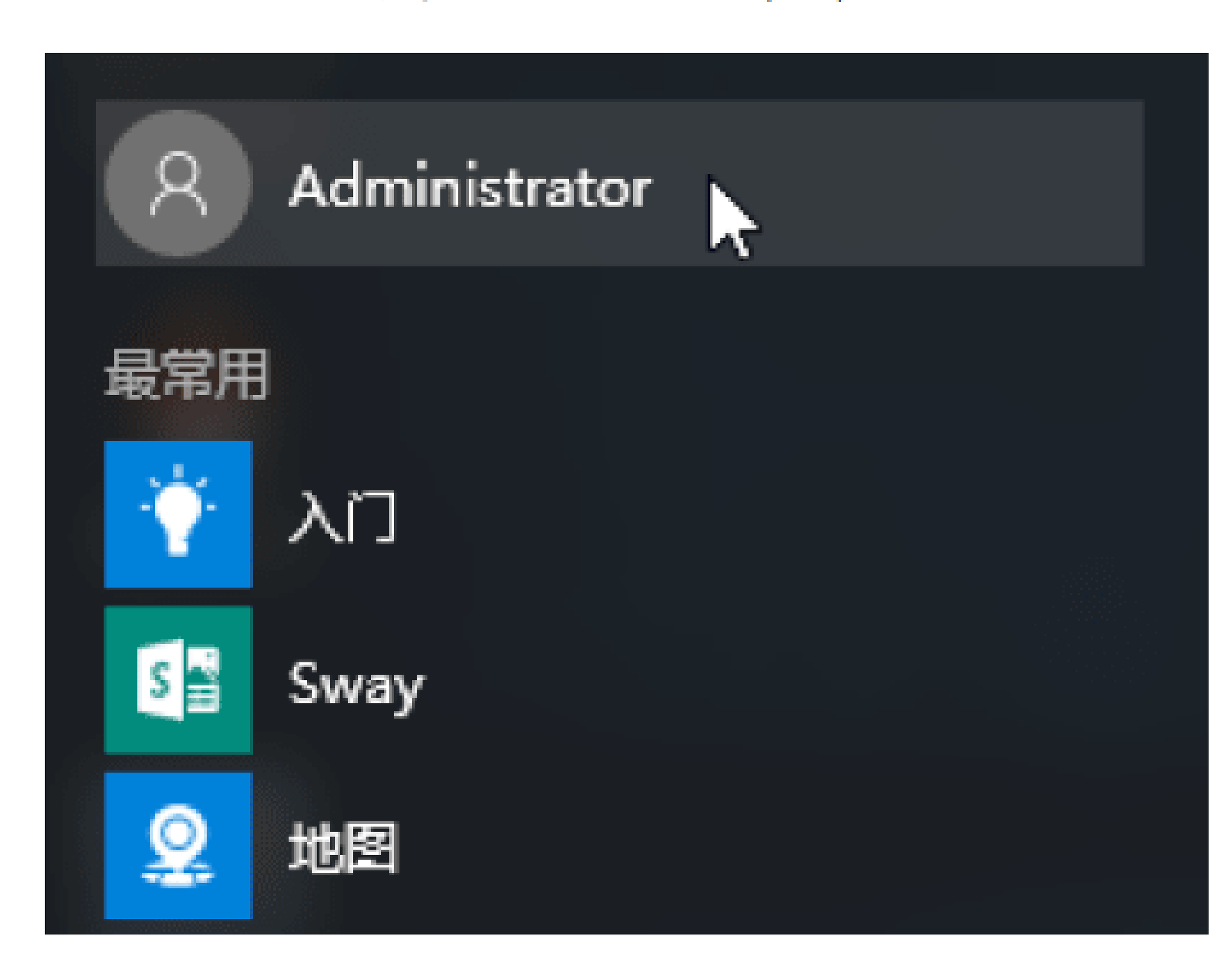
Step 04 打开“Administrator 属性”对话框，在“常规”选项卡中，取消勾选“账户已禁用”复选框，然后单击“确定”按钮，即可启用Administrator账户，如下图所示。



Step 05 单击“开始”按钮，在弹出的面板中单击admini账户，在弹出的下拉面板中可以看到已经启用的Administrator账户，如下图所示。



Step 06 选择Administrator账户登录系统，登录完成后，再单击“开始”按钮，在弹出的面板中可以看到当前登录的账户就是Administrator账户，如下图所示。

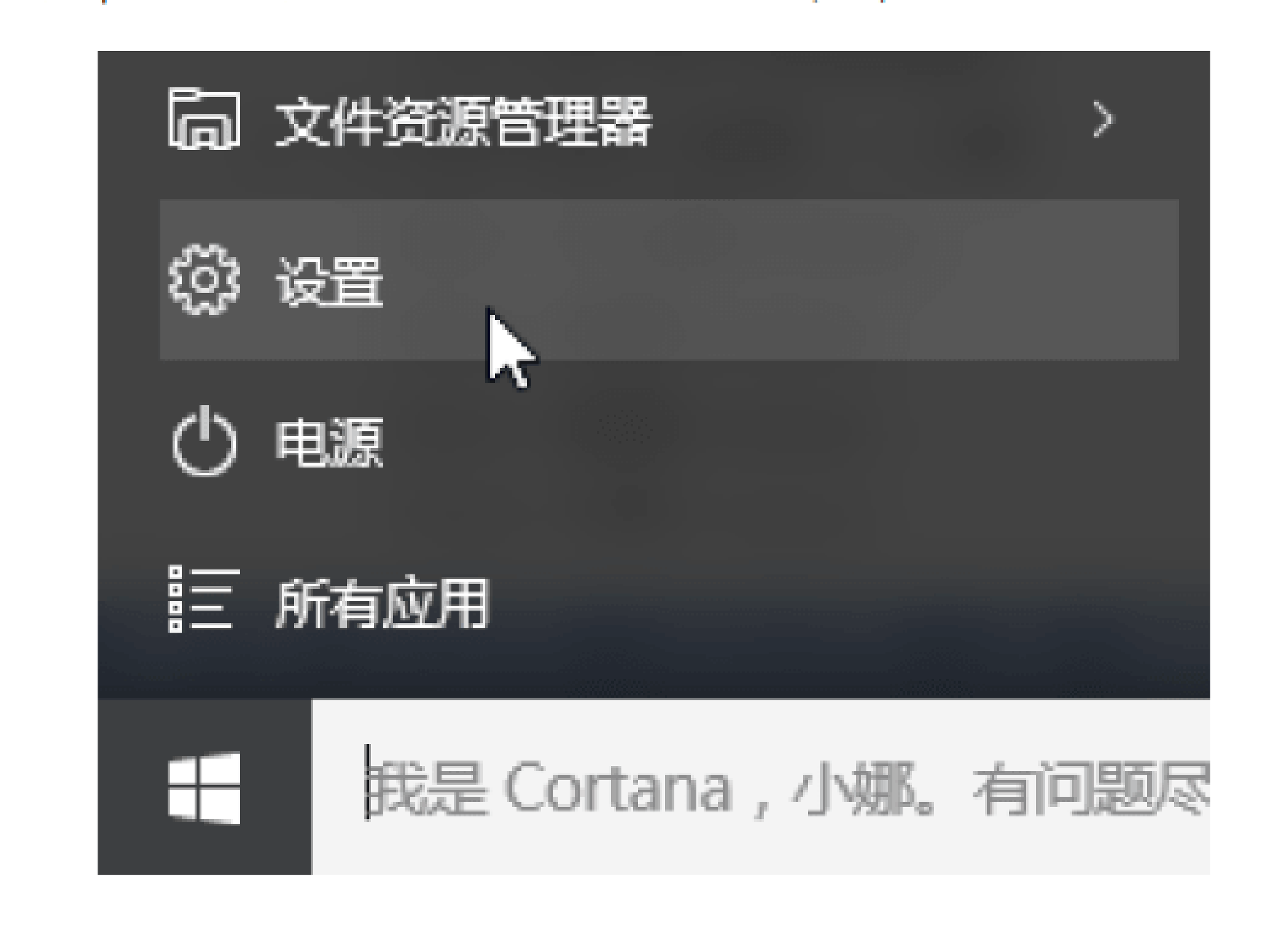


实战4：设置Administrator账户密码

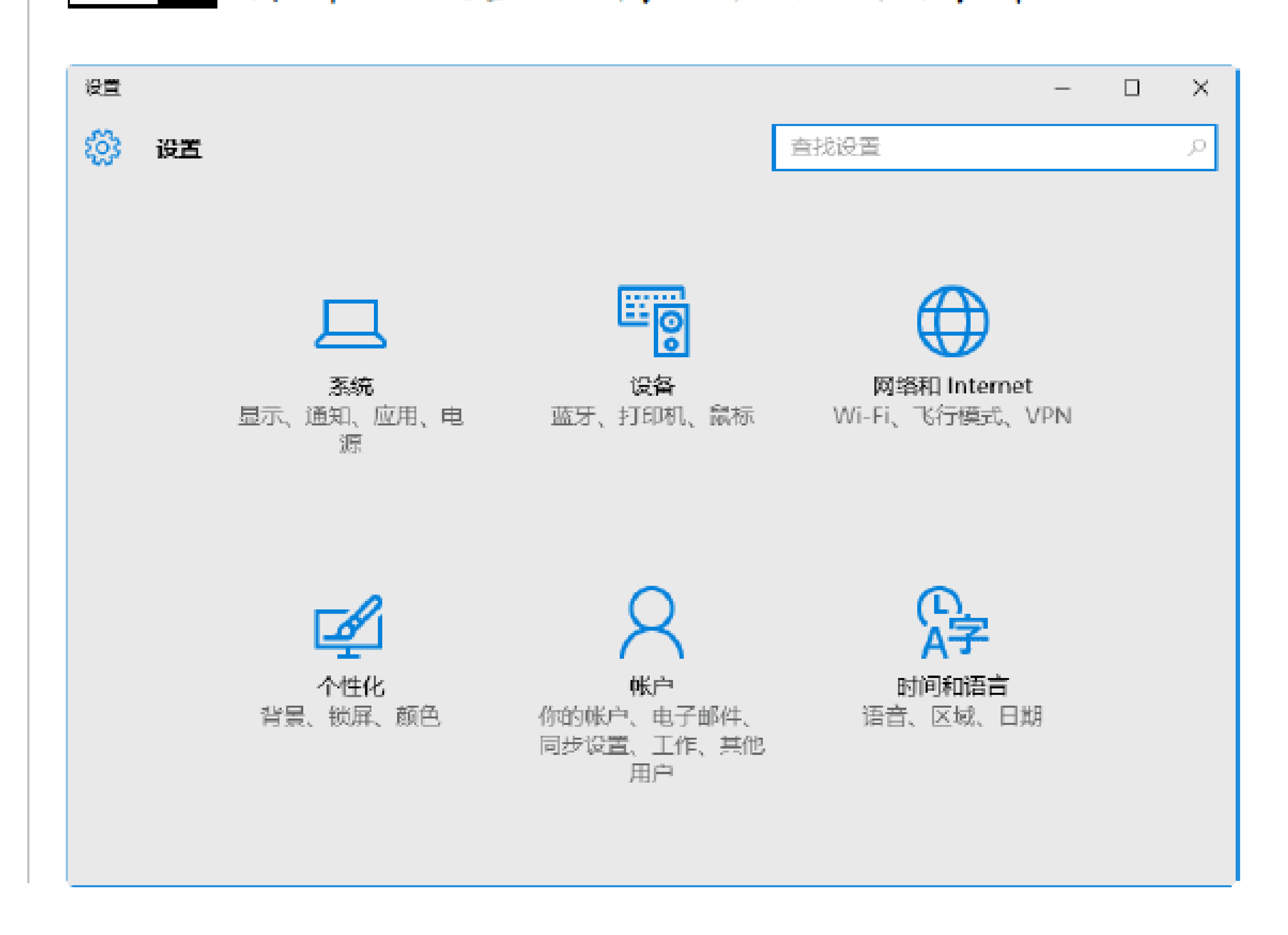


对于添加的账户，用户可以为其创建密码，并对创建的密码进行更改。如果不需要密码，还可以删除账户密码。具体的操作步骤如下。

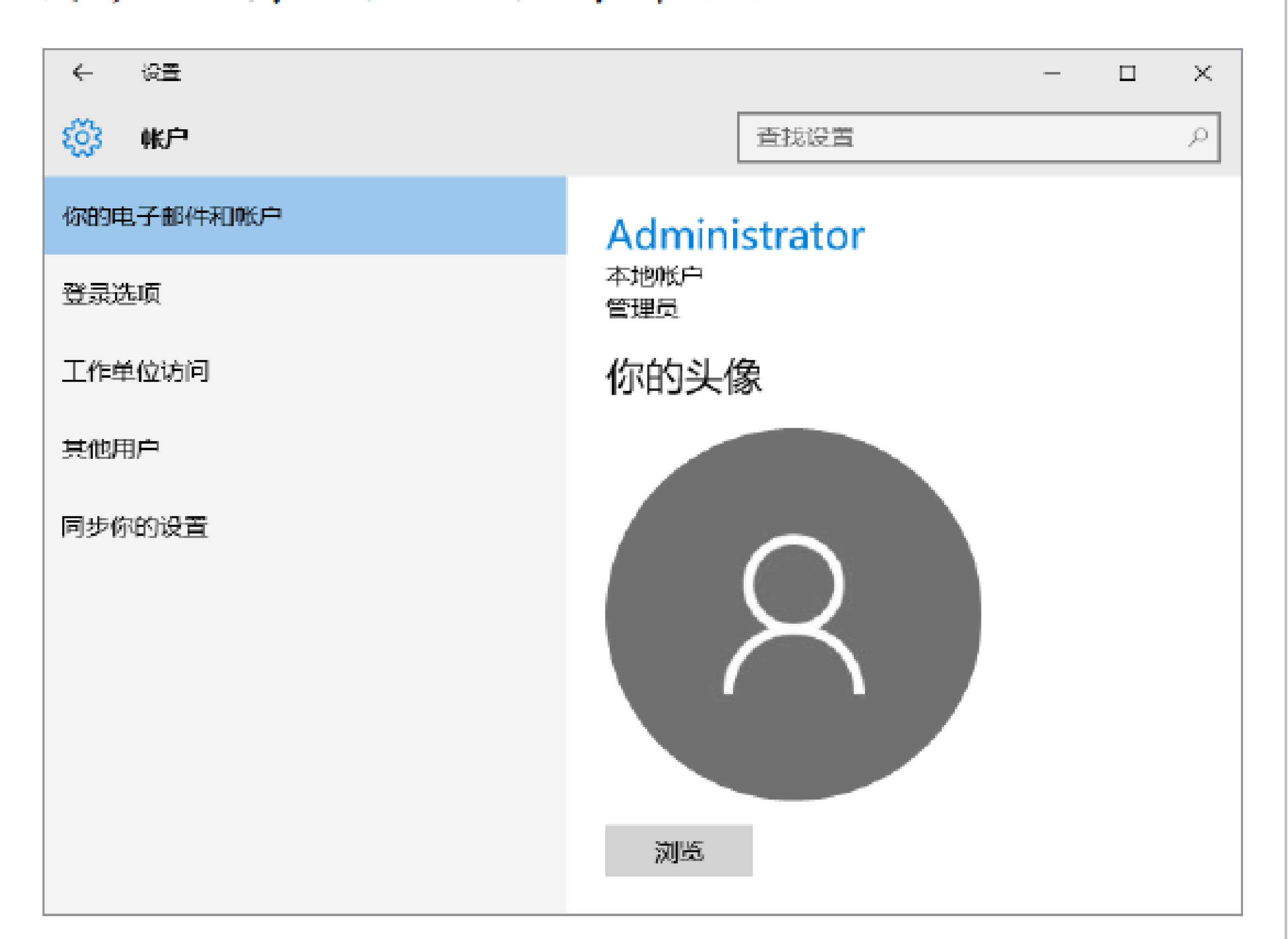
Step 01 单击“开始”按钮，在弹出的面板中选择“设置”选项，如下图所示。



Step 02 打开“设置”窗口，如下图所示。

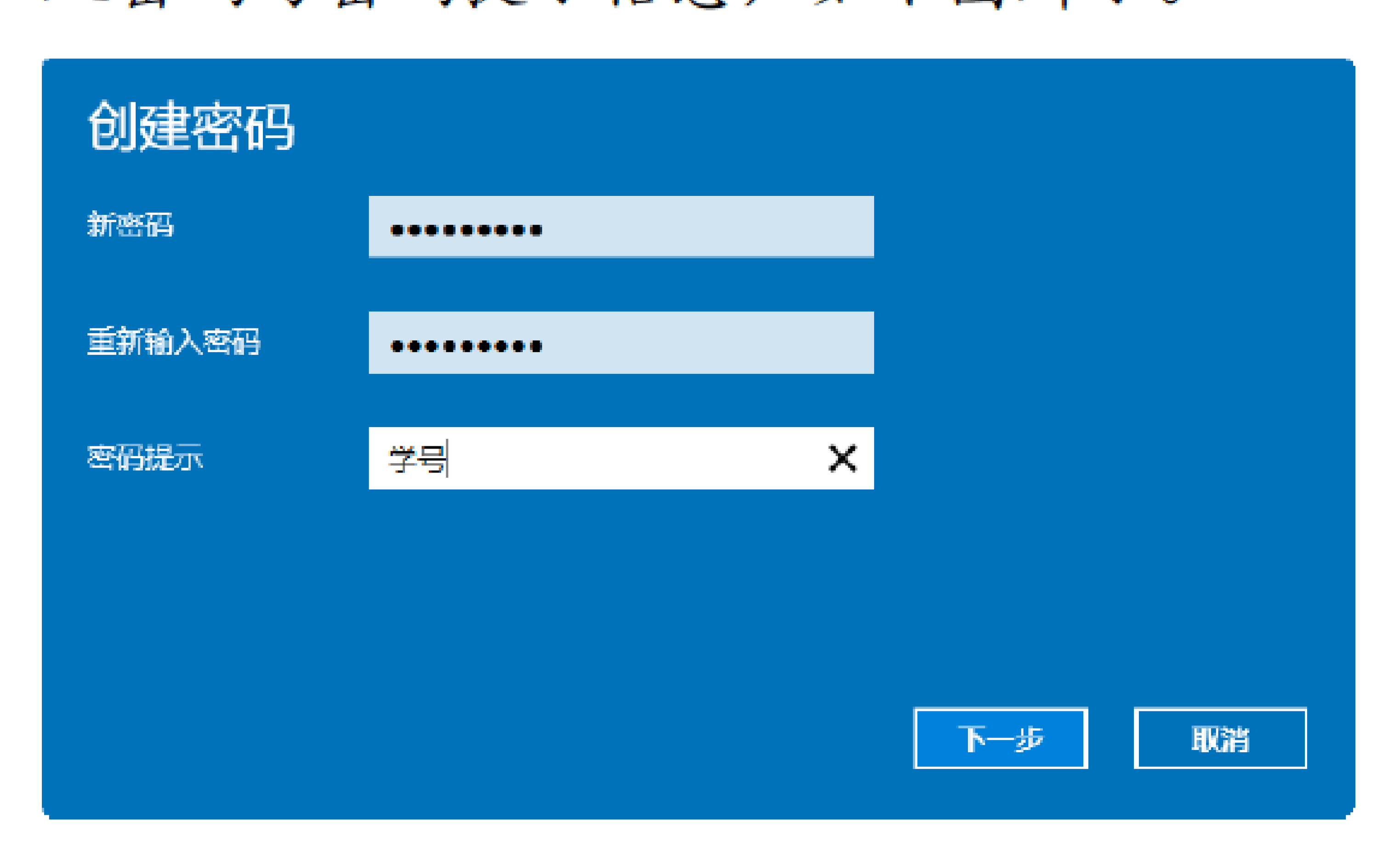


Step 03 单击“账户”超链接，进入“设置-账户”窗口，如下图所示。

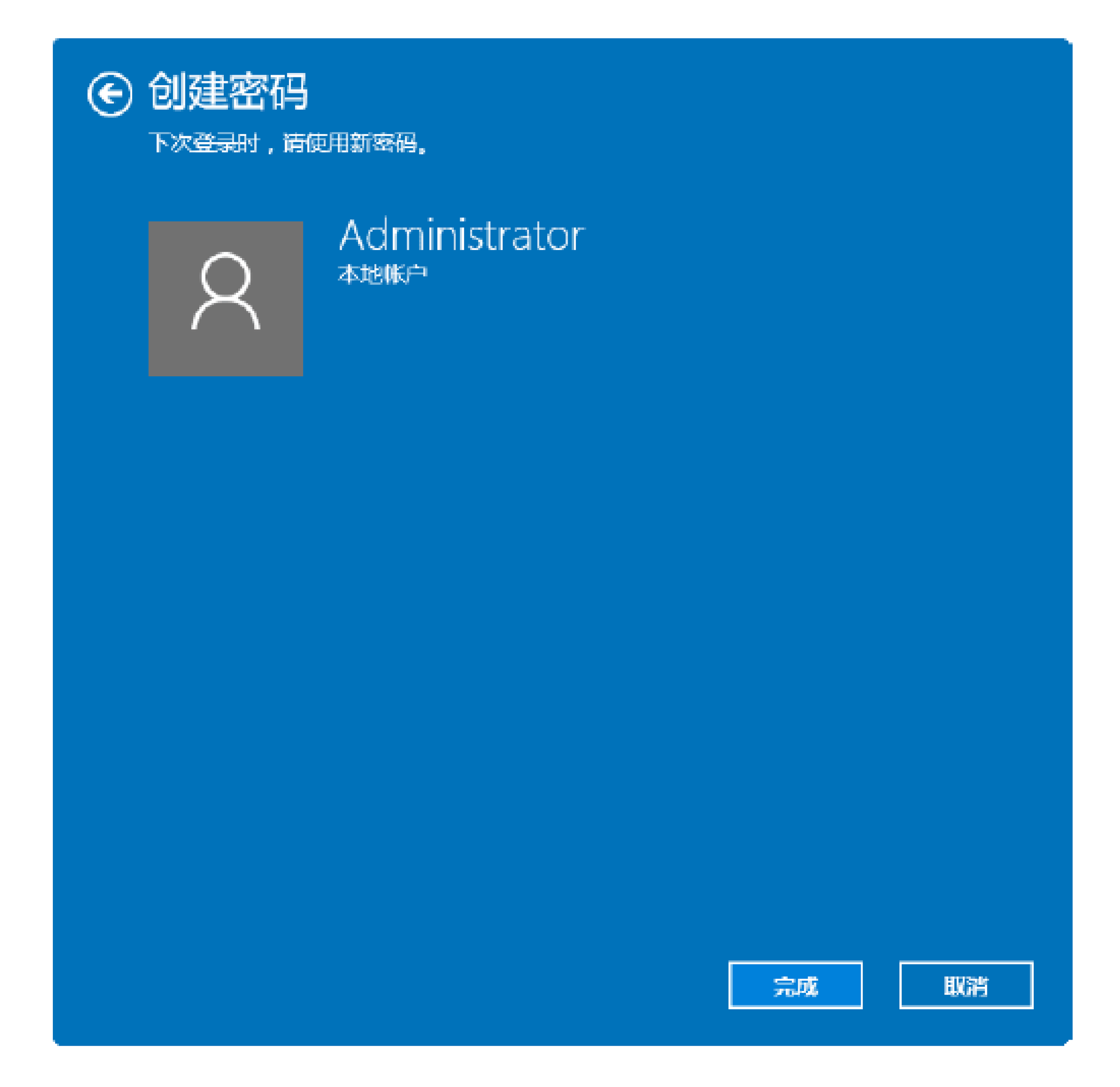


Step 04 选择“登录选项”选项，进入“登录选项”窗口，如下图所示。

Step 05 单击“密码”区域下方的“添加”按钮，打开“创建密码”对话框，在其中输入密码与密码提示信息，如下图所示。



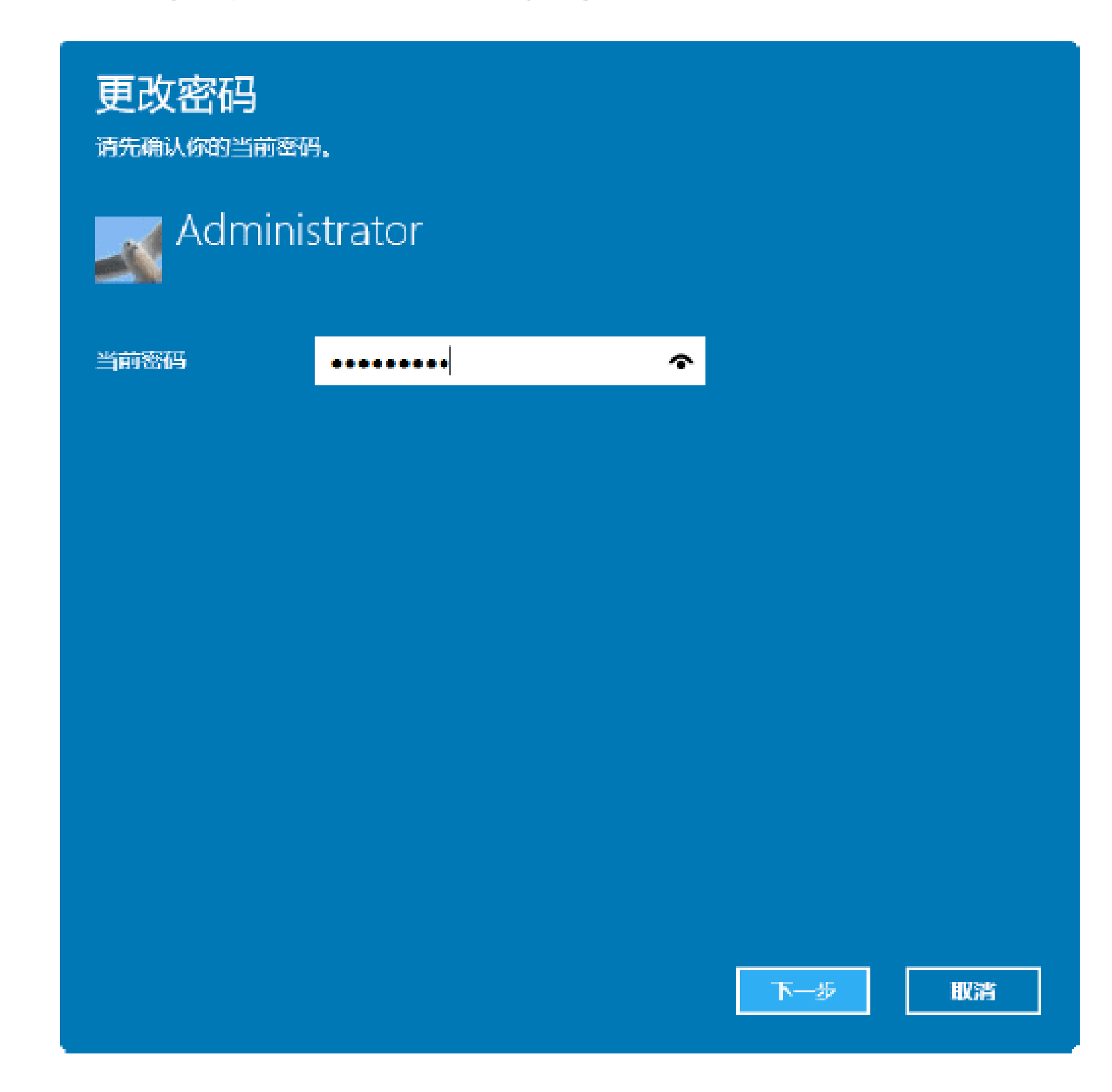
Step 06 单击“下一步”按钮，进入“创建密码”完成界面，设置完成后，提示用户下次登录时，使用新密码，最后单击“完成”按钮，即可完成密码的创建，如下图所示。



Step 07 如果想要更改密码，则需要选择“设置-账户”窗口中的“登录选项”选项，进入“登录选项”设置界面，如下图所示。



Step 08 单击“密码”区域下方的“更改”按钮，打开“更改密码”对话框，在其中输入当前密码，如下图所示。

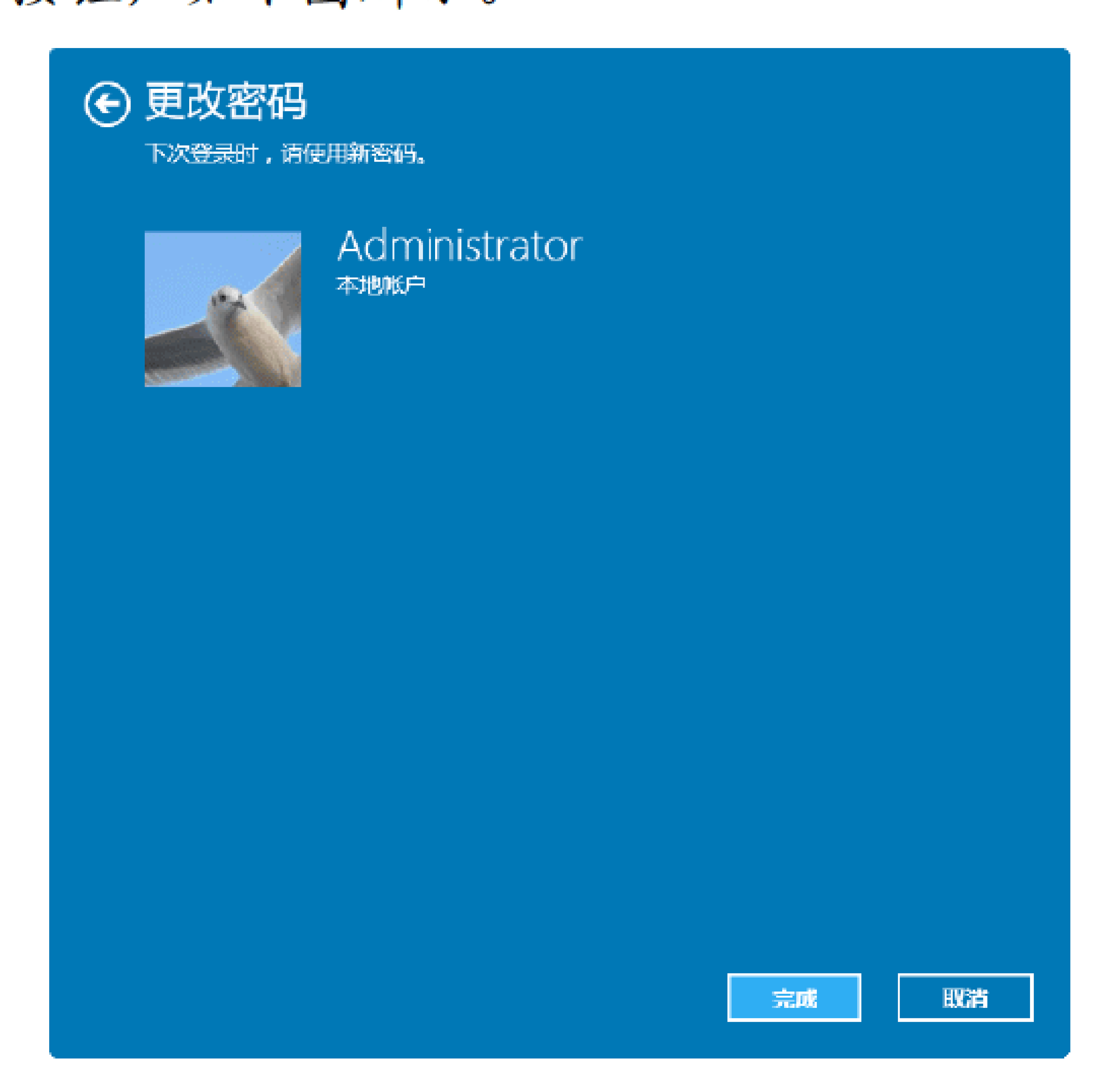


Step 09 单击“下一步”按钮，打开“更改密

码”对话框，在其中输入新密码和密码提示信息，如下图所示。



Step 10 单击“下一步”按钮，即可完成本地账户密码的更改操作，最后单击“完成”按钮，如下图所示。

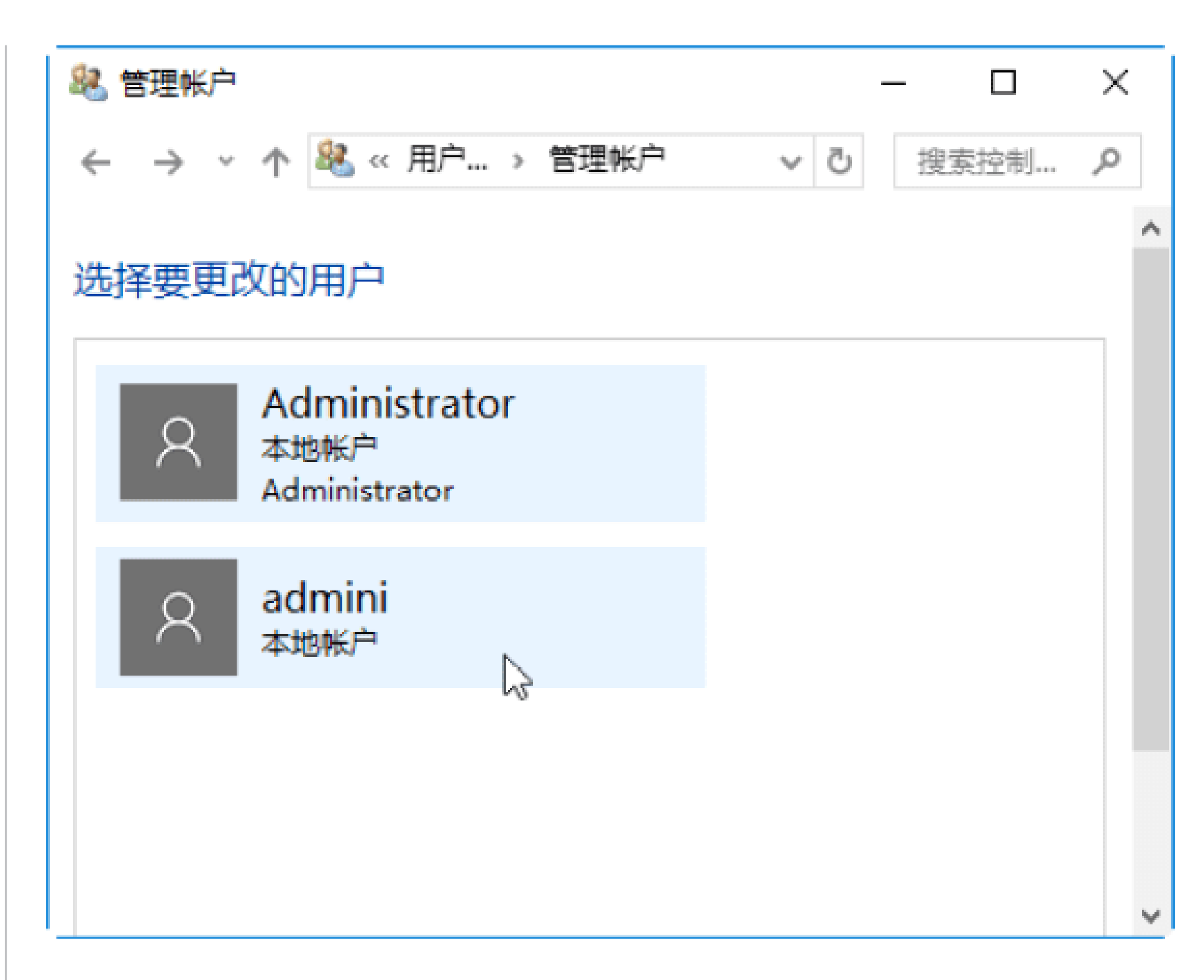


Step 11 如果想要删除密码，则需要在“更改密码”界面中将密码与密码提示设置为空，然后单击“下一步”按钮，即可完成删除密码操作。

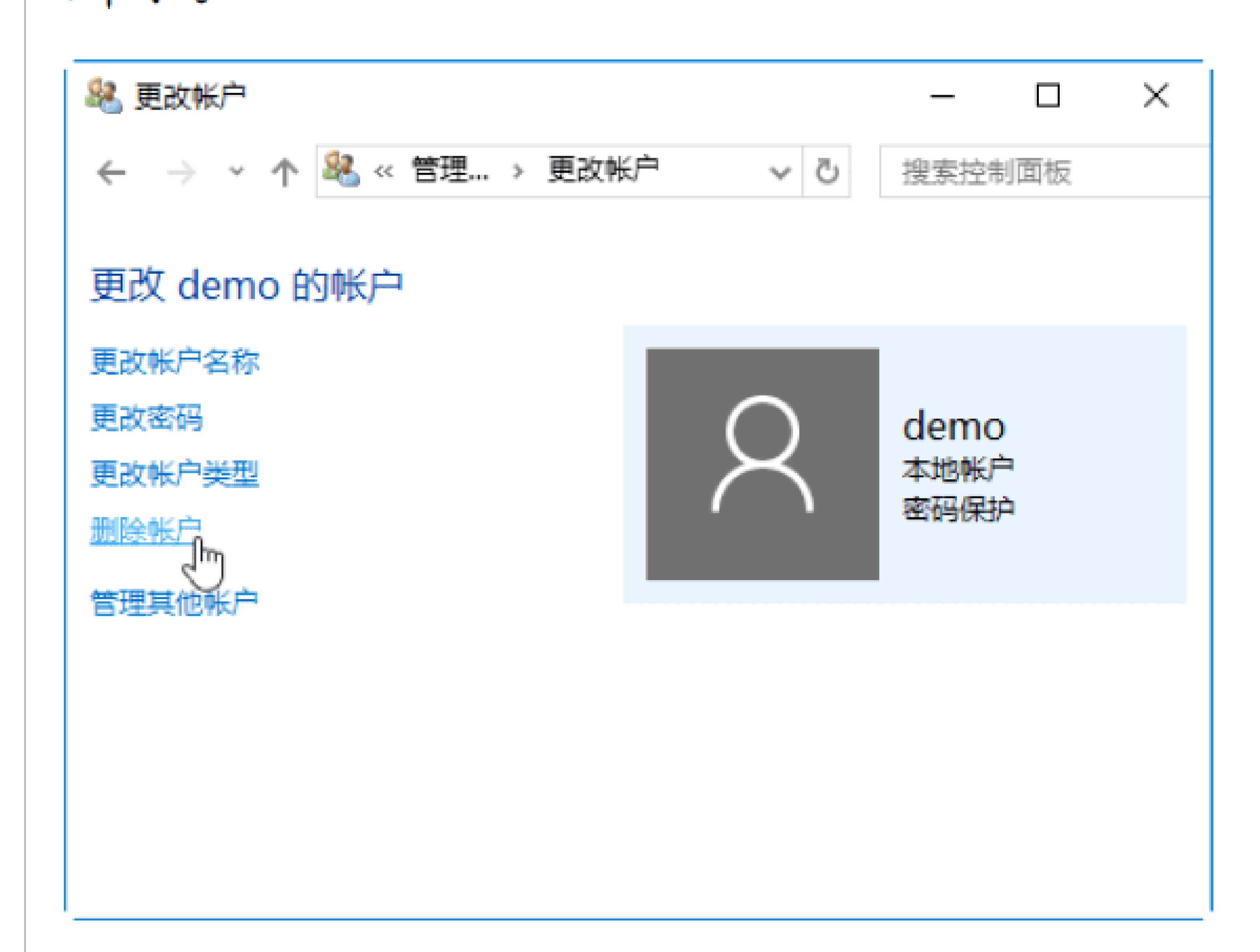
实战5：删除不需要的本地用户账户

对于不需要的本地账户，用户可以将其删除，具体的操作步骤如下。

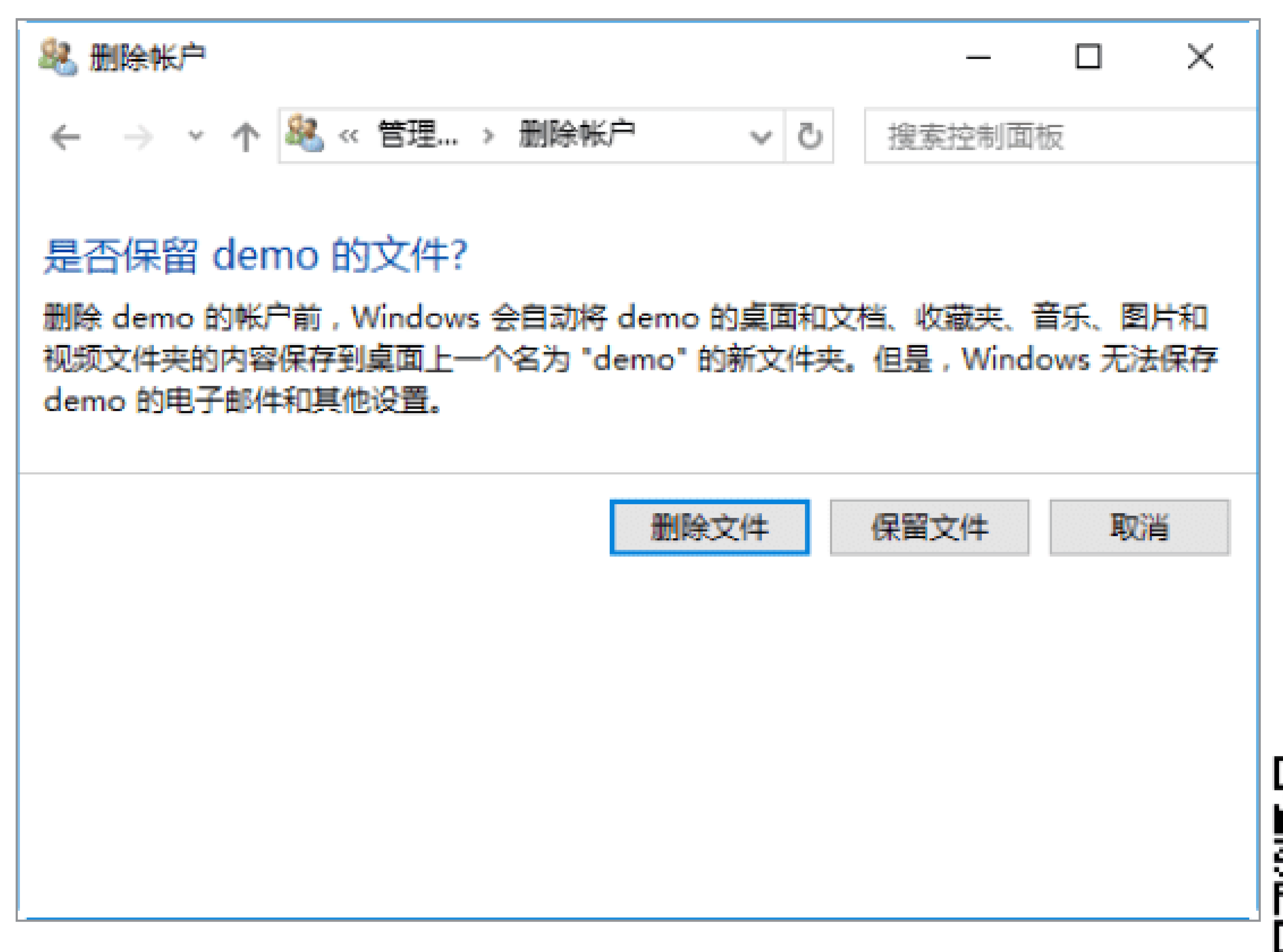
Step 01 打开“管理账户”窗口，在其中选择要删除的账户，如下图所示。



Step 02 进入“更改账户”窗口，在其中单击左侧的“删除账户”超链接，如下图所示。

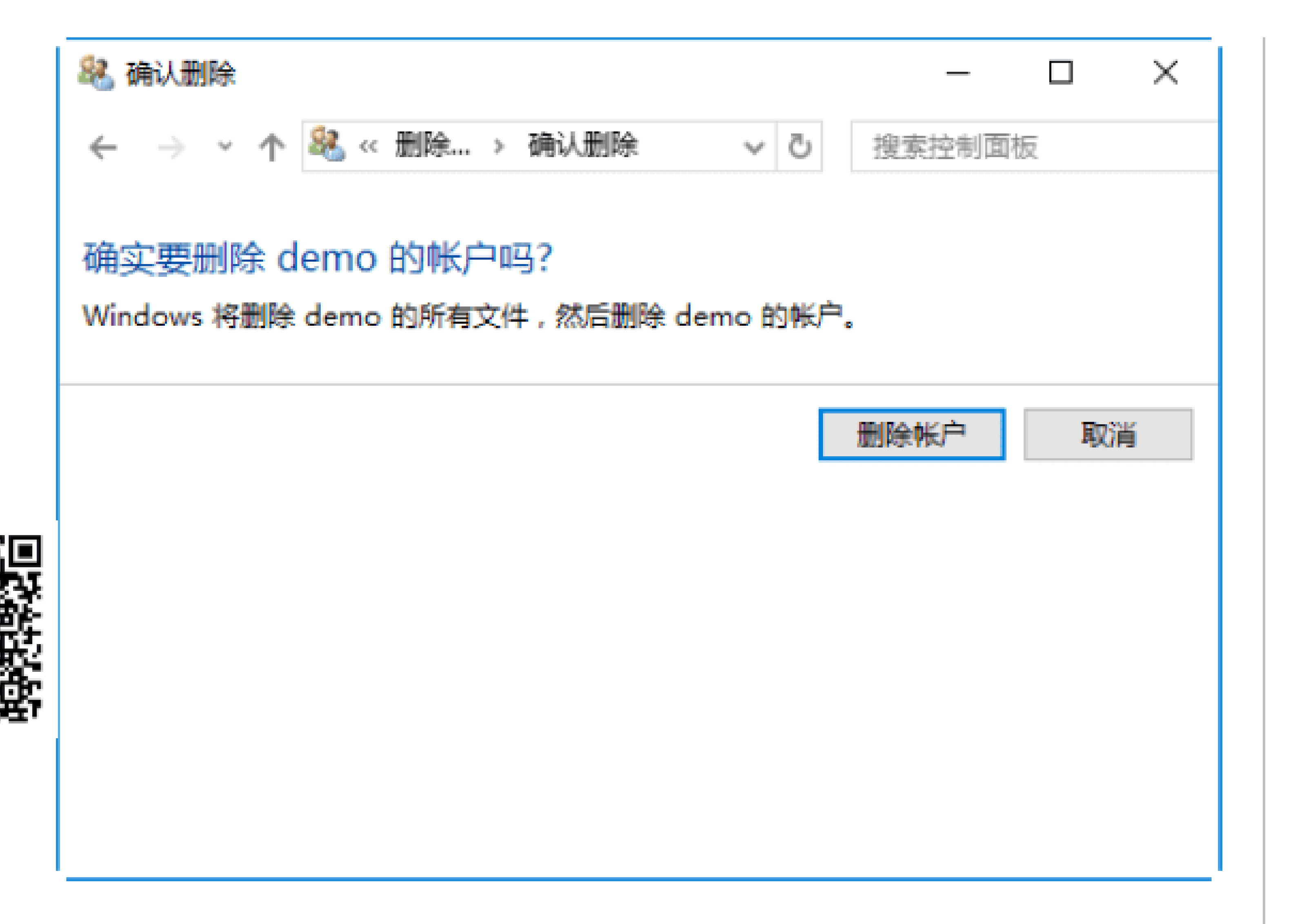


Step 03 进入“删除账户”窗口，提示用户是否保存账户的文件，如下图所示。

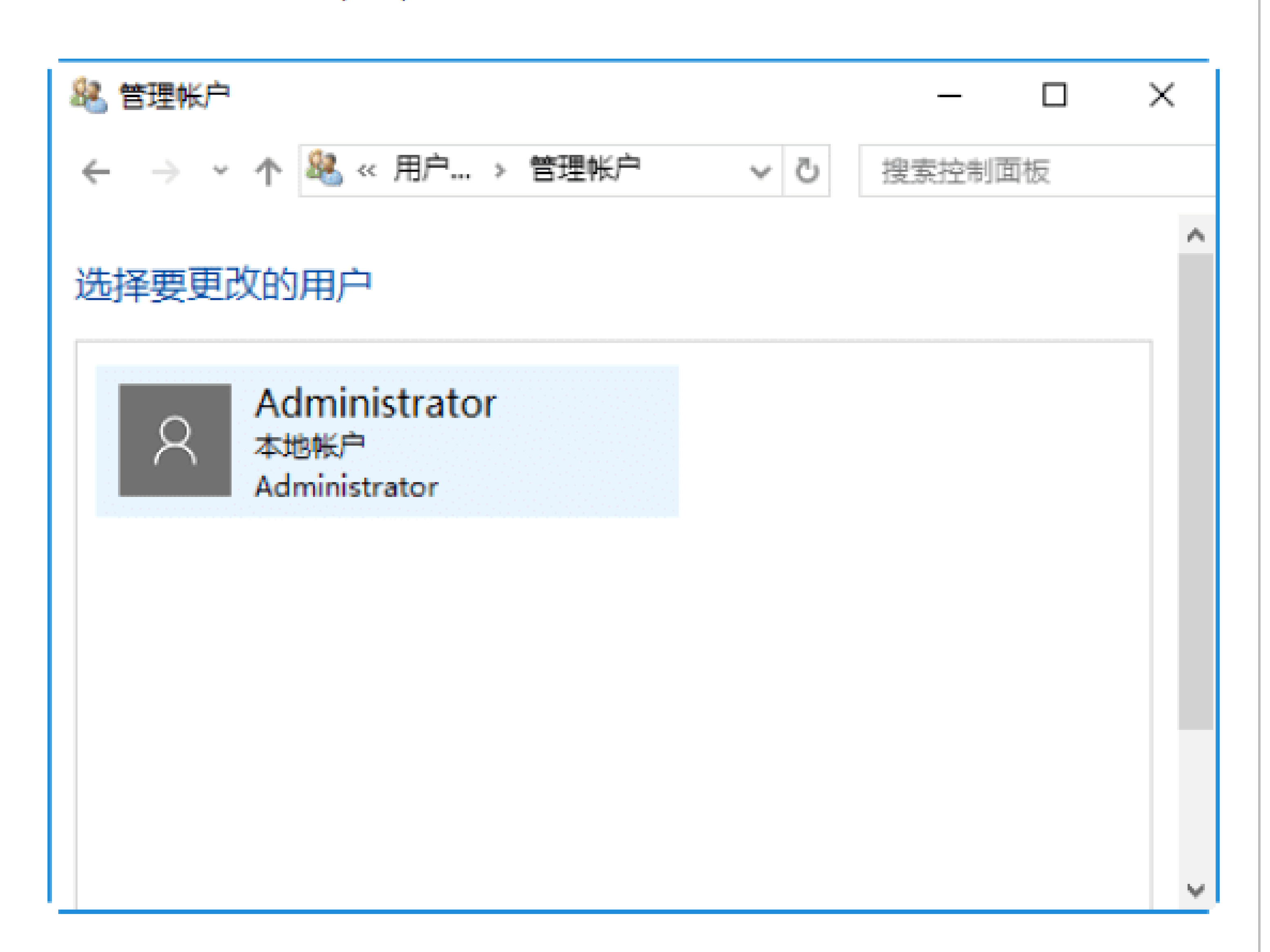




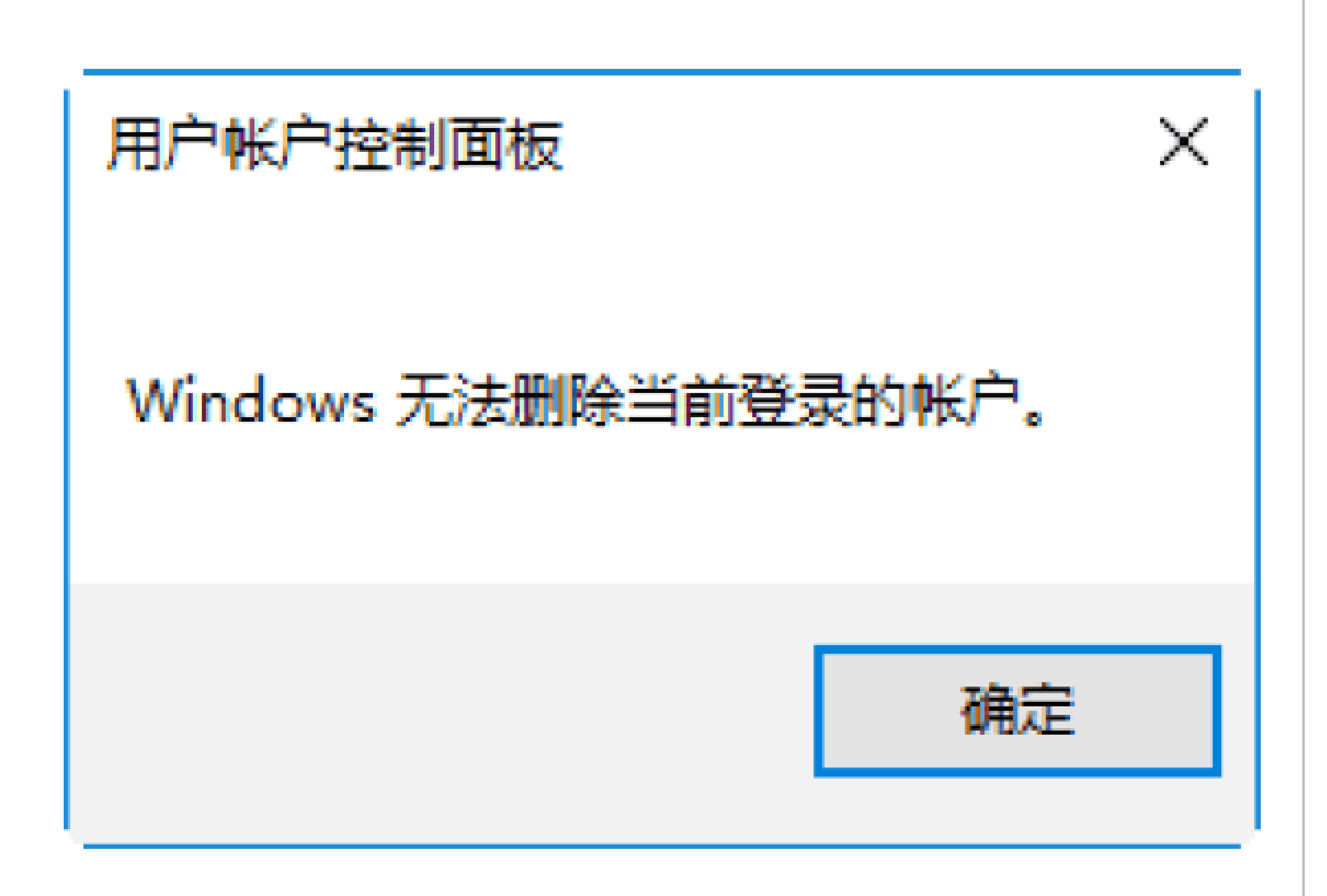
Step 04 单击“删除文件”按钮，进入“确认删除”窗口，提示用户是否确实要删除demo账户，如下图所示。



Step 05 单击“删除账户”按钮，即可删除选择的账户，并返回到“管理账户”窗口，在其中可以看到删除的账户已经不存在了，如下图所示。



提示：对于当前正在登录的账户，Windows是无法删除的，因此，在删除账户的过程中，会弹出一个“用户账户控制面板”信息提示框，用于提示用户，如下图所示。



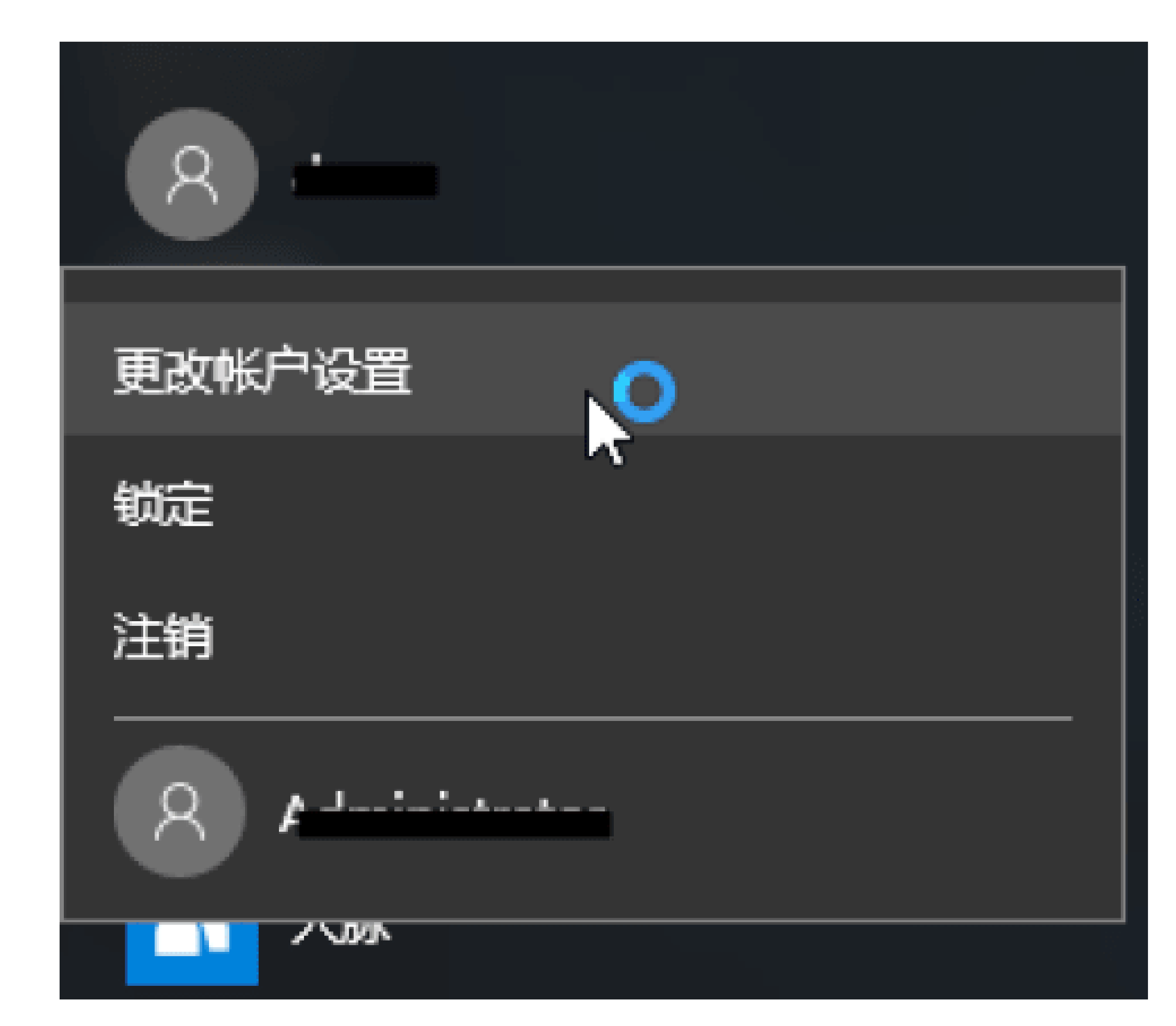
5.4　Microsoft账户的安全防护

Microsoft账户是用于登录Windows的电子邮件地址和密码组合，本节介绍Microsoft账户的设置与应用，从而保护计算机系统。

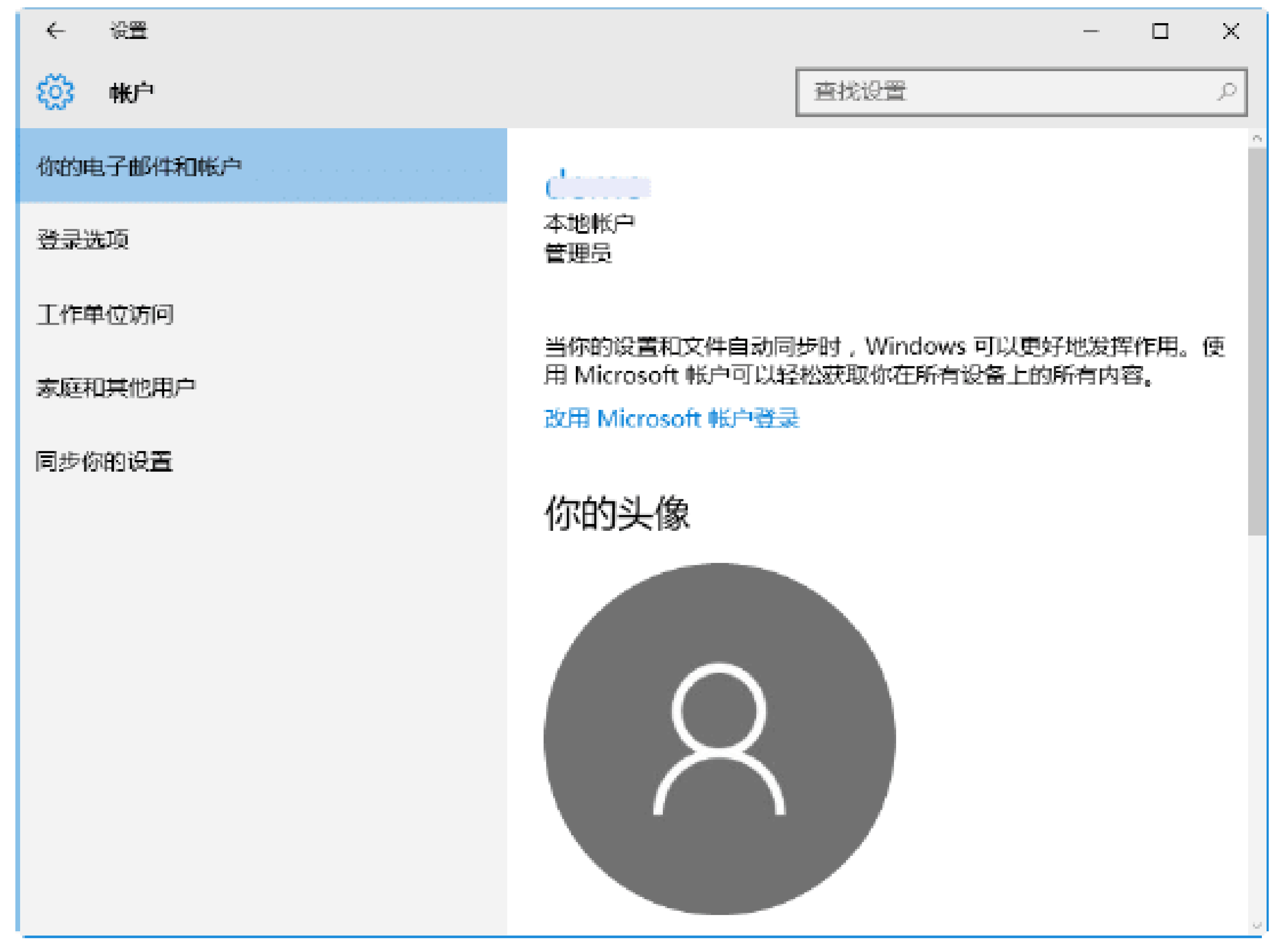
实战6：注册并登录Microsoft账户

要想使用Microsoft账户管理此设备，首先需要做的就是在此设备上注册并登录Microsoft账户。注册并登录Microsoft账户的操作步骤如下。

Step 01 单击“开始”按钮，在弹出的界面中单击要登录的账户，在弹出的下拉列表中选择“更改账户设置”选项，如下图所示。



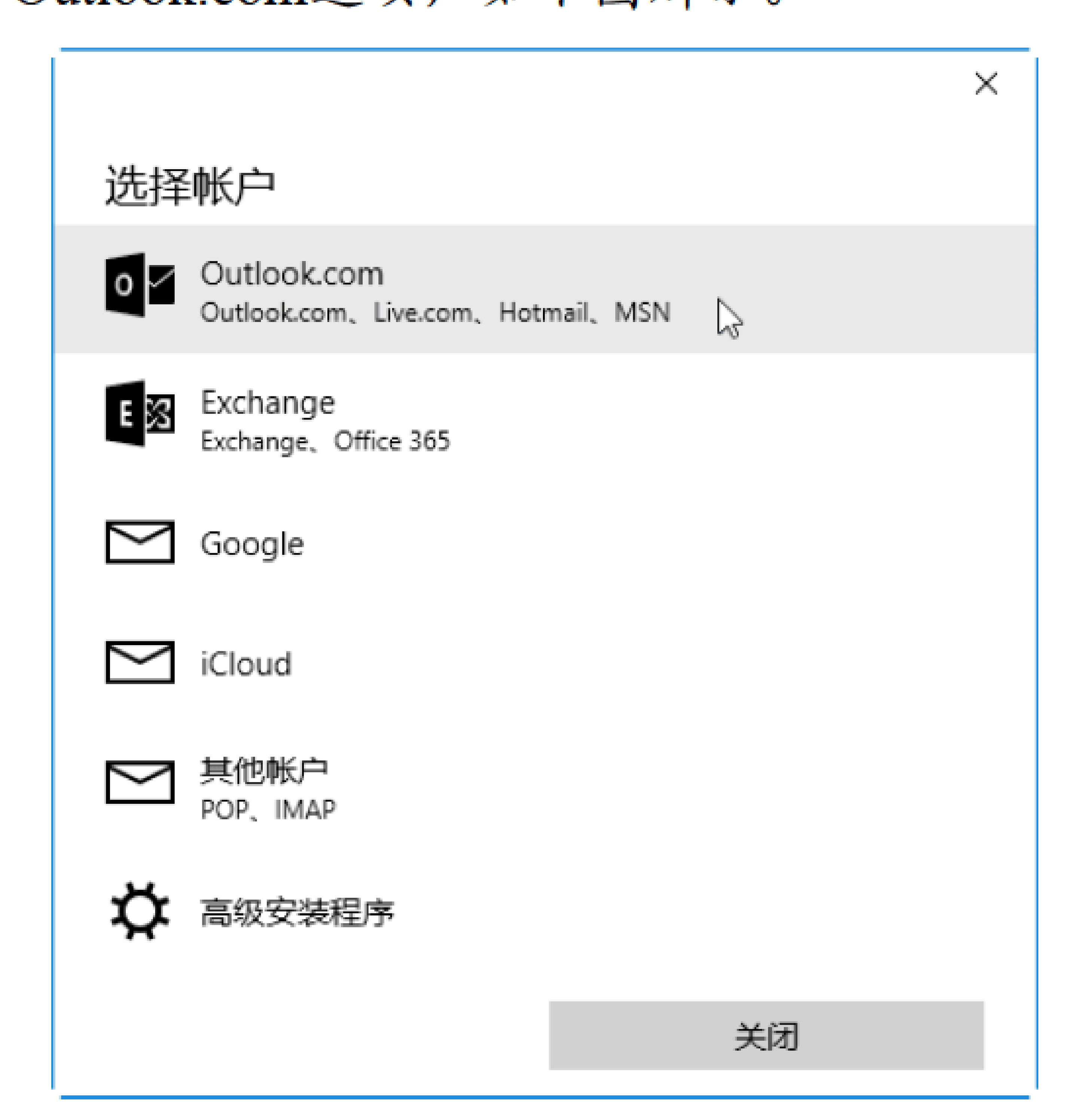
Step 02 打开“设置-账户”窗口，在其中选择“你的电子邮件和账户”选项，如下图所示。



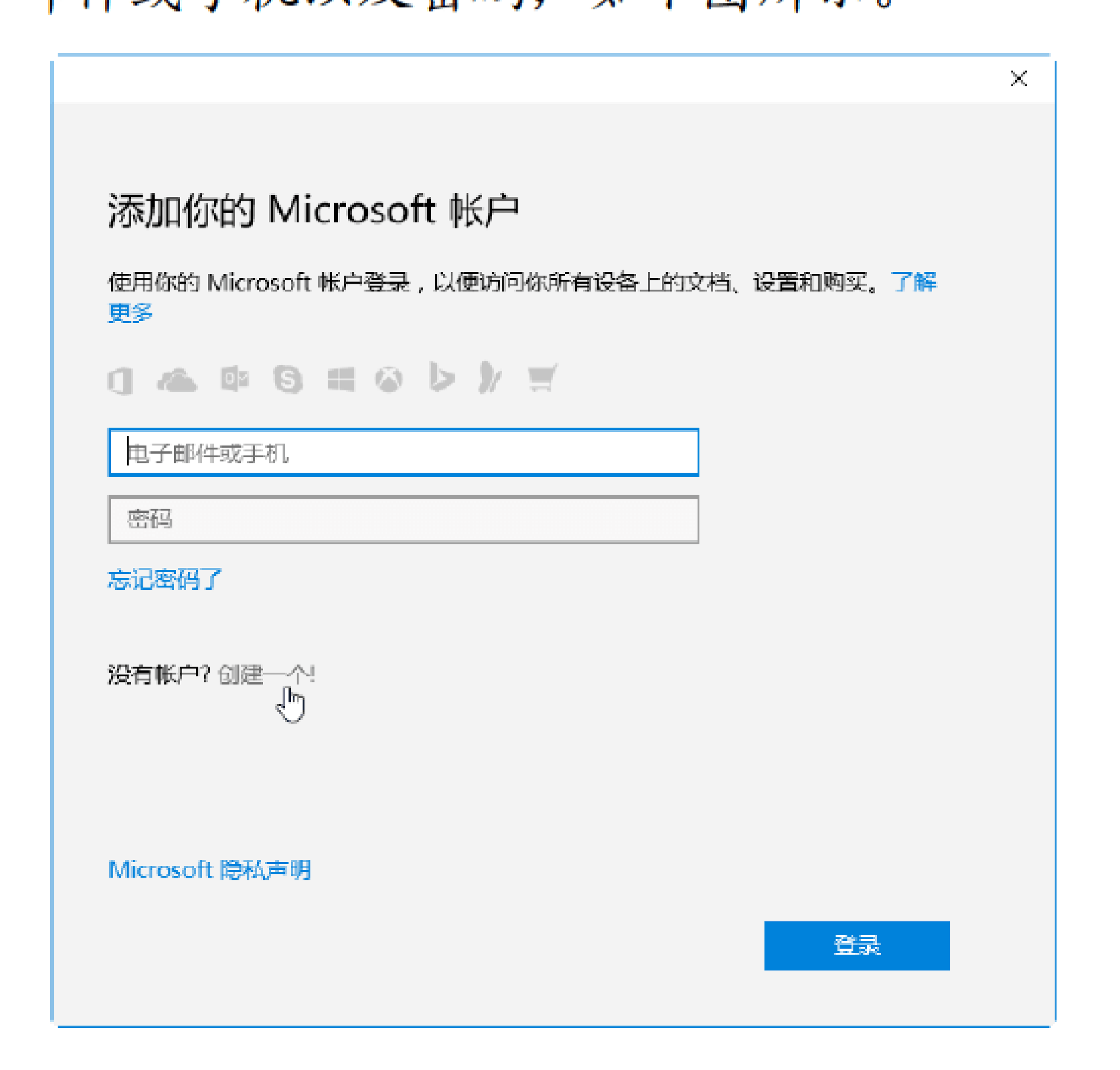
Step 03 单击“电子邮件、日历和联系人”下方的“添加账户”选项，如下图所示。



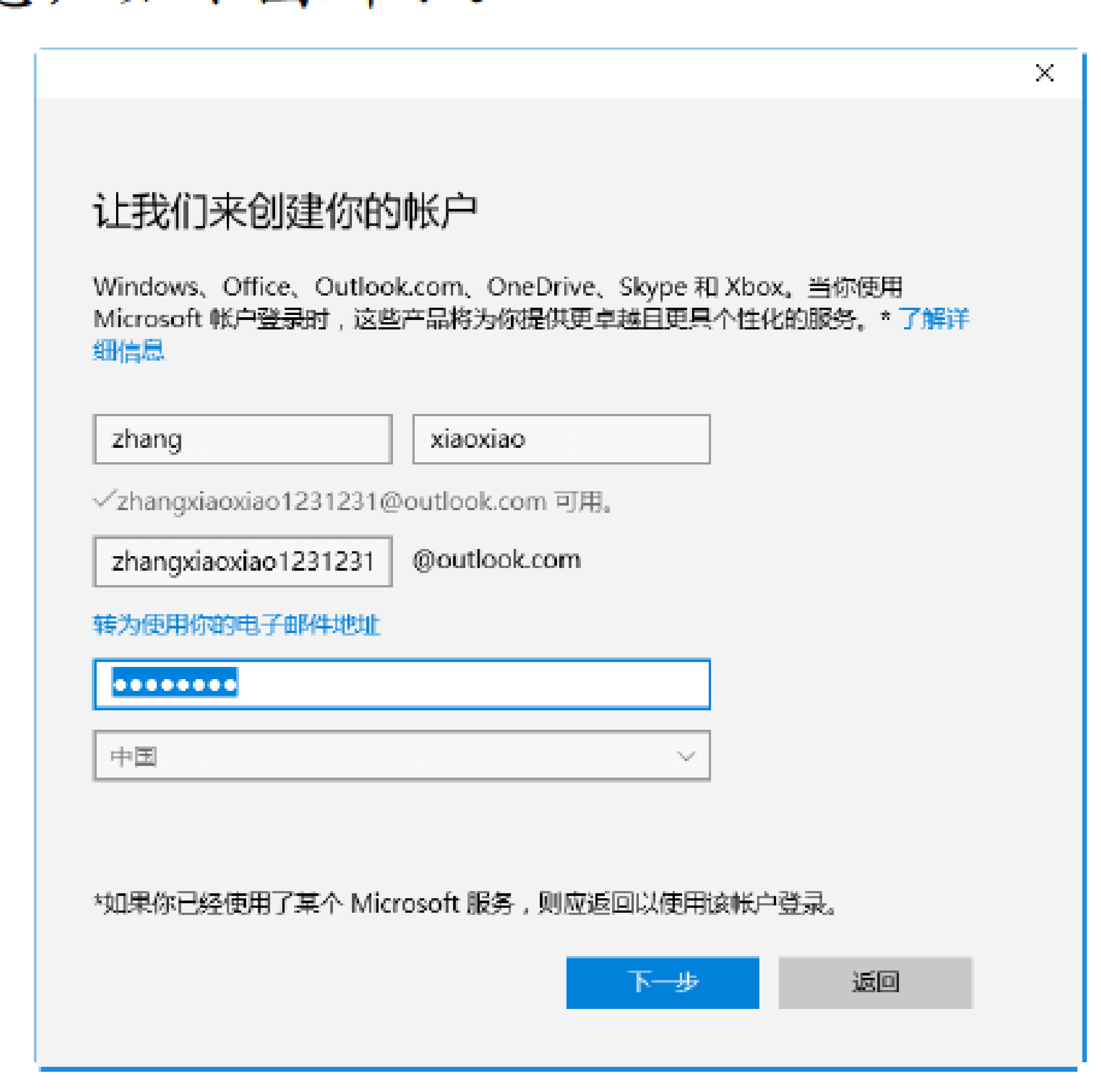
Step 04 弹出“选择账户”列表，在其中选择Outlook.com选项，如下图所示。



Step 05 打开“添加你的Microsoft账户”对话框，在其中可以输入Microsoft账户的电子邮件或手机以及密码，如下图所示。



Step 06 如果没有Microsoft账户，则需要单击“创建一个！”超链接，打开“让我们来创建你的账户”对话框，在其中输入账户信息，如下图所示。



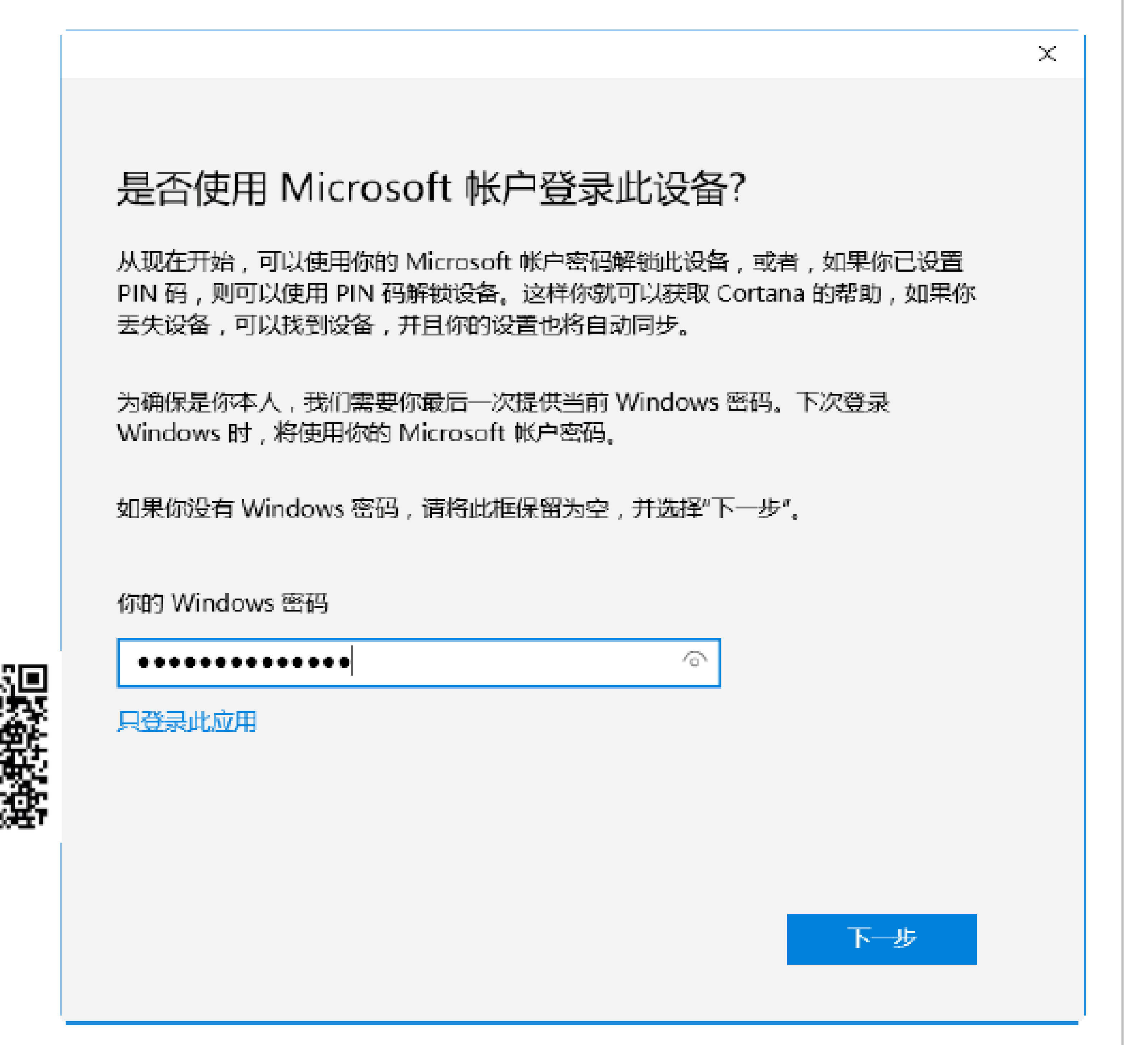
Step 07 单击“下一步”按钮，打开“添加安全信息”对话框，在其中输入手机号码，如下图所示。

添加安全信息
你的安全信息有助于保护你的帐户。我们将使用此信息来帮助你恢复密码、帮助保护你的帐户免受黑客侵袭，并在你遇到故障时让你恢复正常状态。我们不会利用它来发送垃圾邮件。
中国 (+86)
[redacted]
改为添加备选电子邮件
下一步
返回

Step 08 单击“下一步”按钮，打开“查看与你相关度最高的内容”对话框，在其中查看相关说明信息，如下图所示。

查看与你相关度最高的内容
当 Microsoft 通过使用你的首选项以及分析你的数据来对你的体验进行个性化定制时，请确保你能看到你最喜欢的搜索结果、广告，以及其他内容。你可以在线更改这些设置，也可以在某些 Microsoft 产品和服务中进行更改。
允许 Microsoft Advertising 使用我的帐户信息，使我的在线体验更完美。(你可以随时更改此设置。)
向我发送 Microsoft 促销优惠信息。(你可以随时取消订阅。)
单击“下一步”表示你同意 Microsoft 服务协议和隐私和 cookie 声明。
下一步
返回

Step 09 单击“下一步”按钮，打开“是否使用Microsoft账户登录此设备？”对话框，在其中输入Windows密码，如下图所示。



Step 10 单击“下一步”按钮，打开“全部完成”对话框，提示用户账户已经成功设置，如下图所示。

全部完成!

你的帐户已成功设置。

zhangxiaoxiao1231231@outlook.com

完成

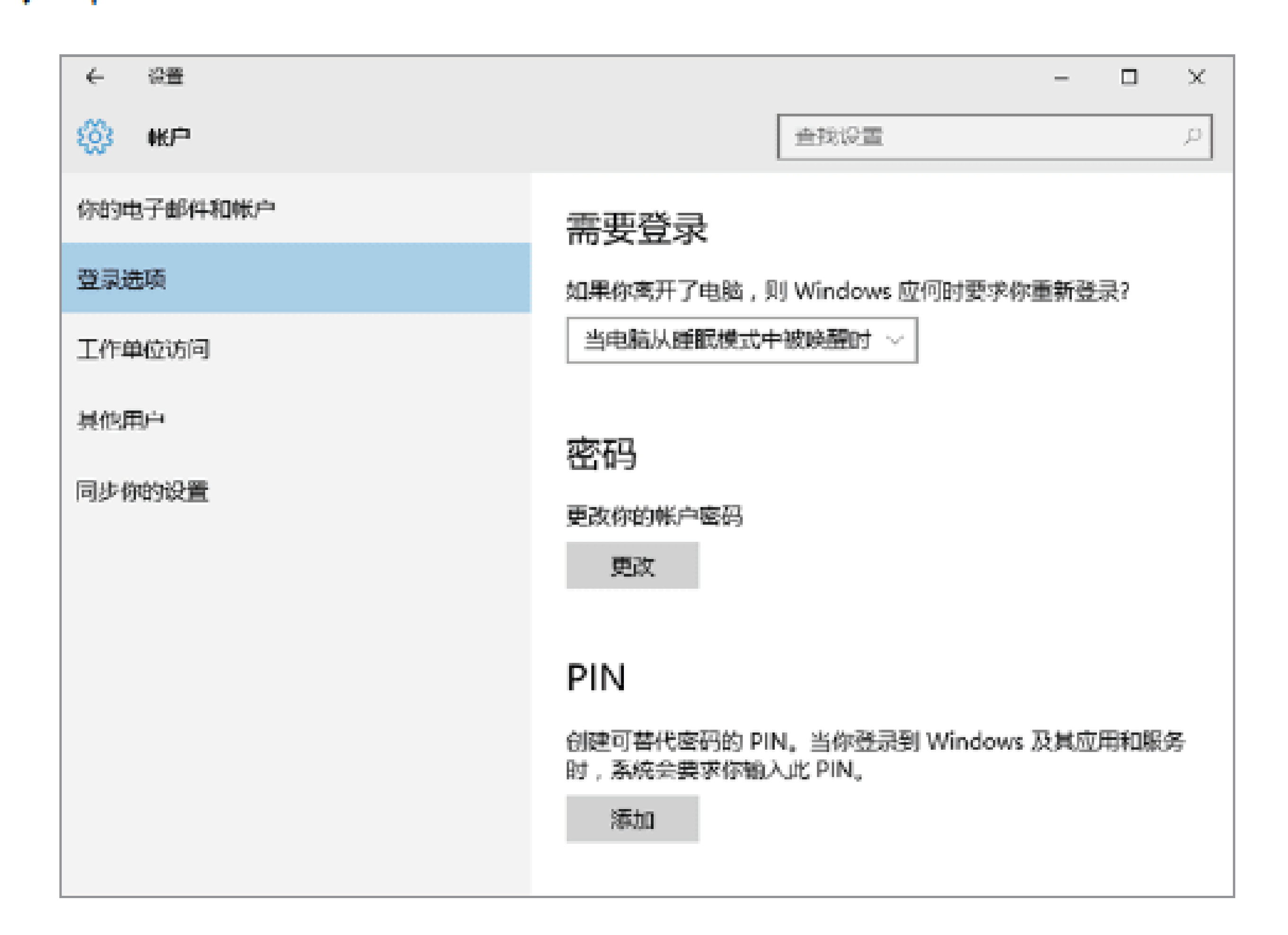
Step 11 单击“完成”按钮，即可使用Microsoft账户登录到本台计算机上，至此，就完成了Microsoft账户的注册与登录操作，如下图所示。



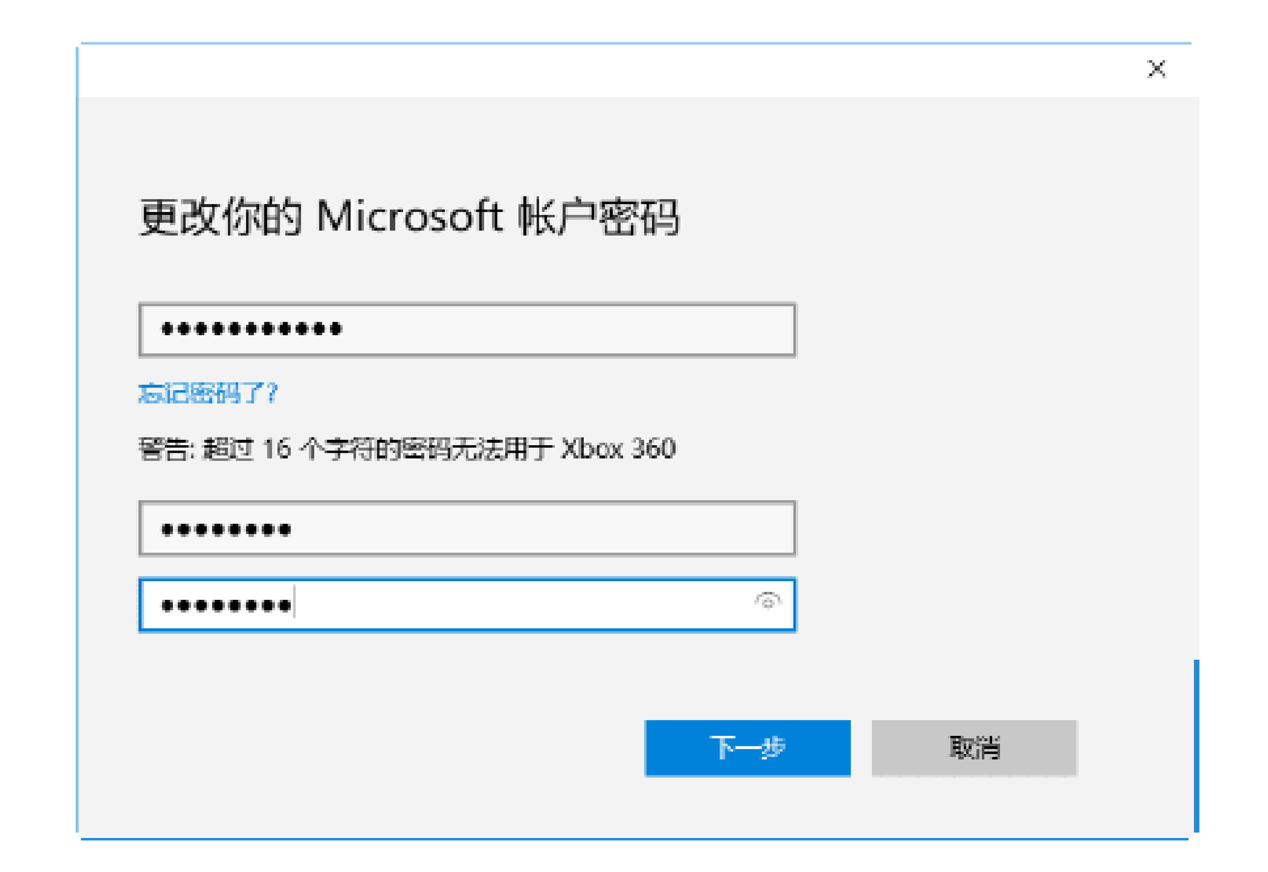
实战7：设置Microsoft账户登录密码

为账户设置登录密码，在一定程度上保护计算机的安全。为Microsoft账户设置登录密码的操作步骤如下。

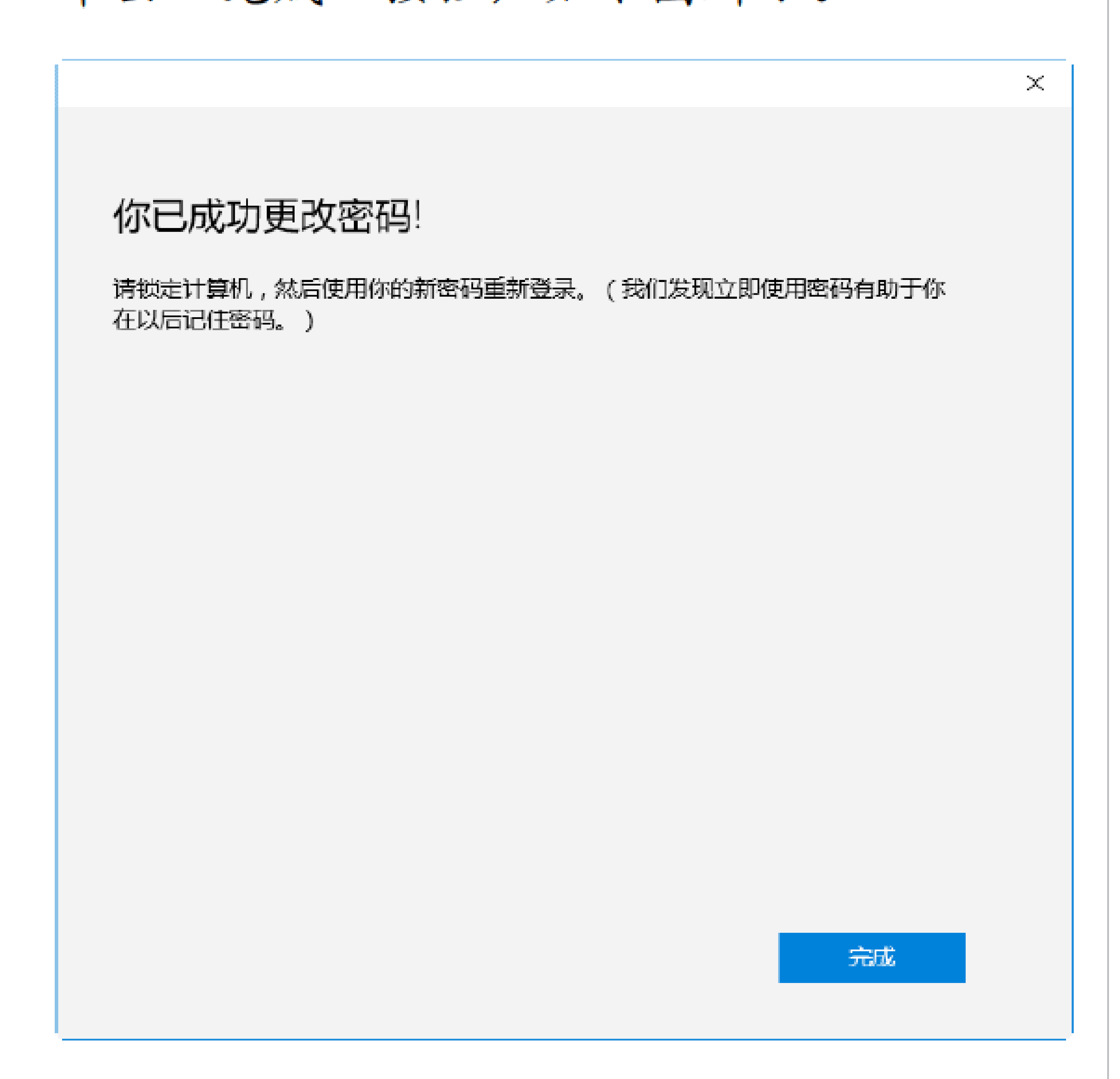
Step 01 以Microsoft账户类型登录本台设备，选择“设置-账户”窗口中的“登录选项”选项，进入“登录选项”设置界面，如下图所示。



Step 02 单击“密码”区域下方的“更改”按钮，打开“更改你的Microsoft账户密码”对话框，在其中输入当前密码和新密码，如下图所示。



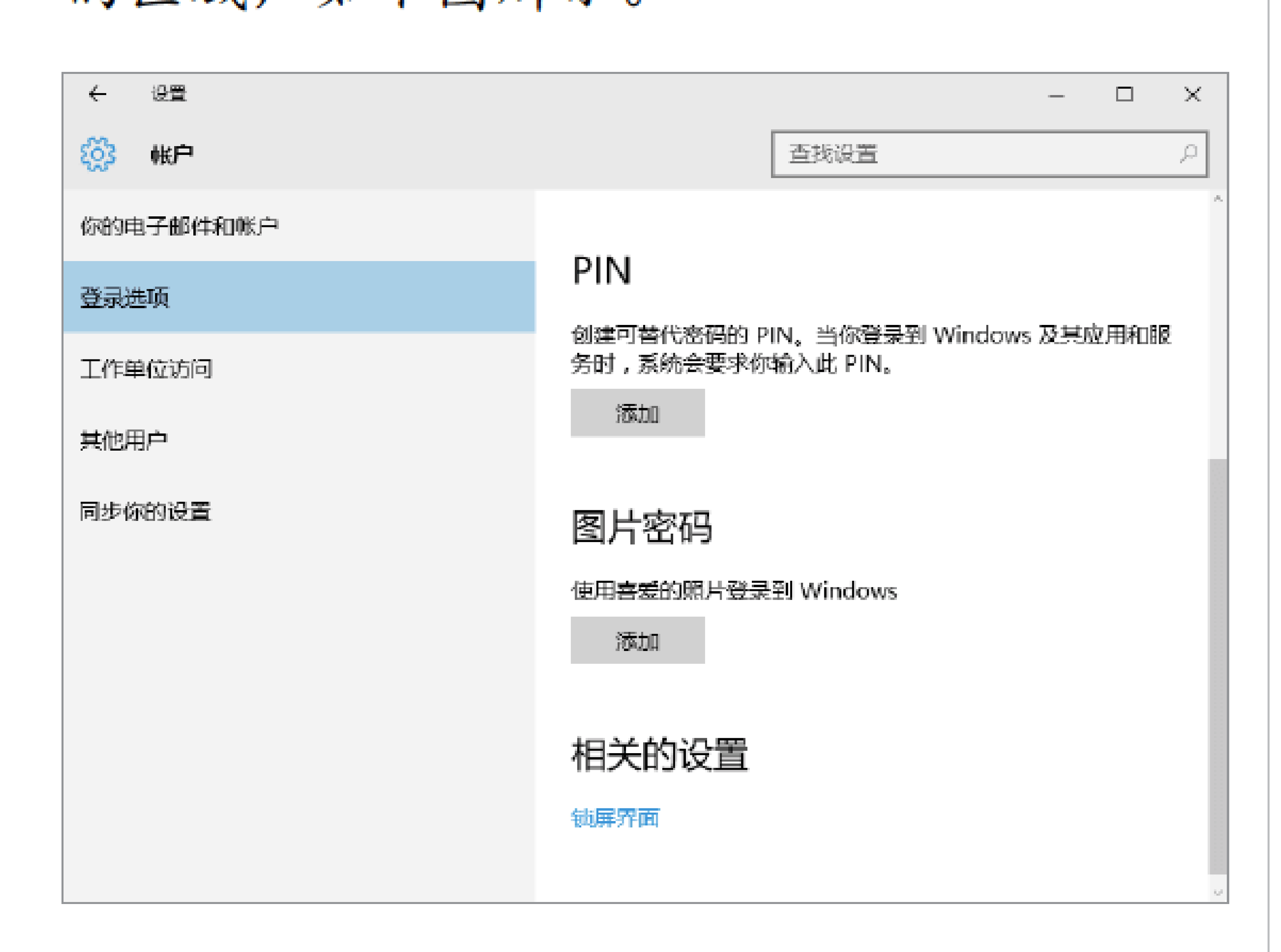
Step 03 单击“下一步”按钮，即可完成Microsoft账户登录密码的更改操作，最后单击“完成”按钮，如下图所示。



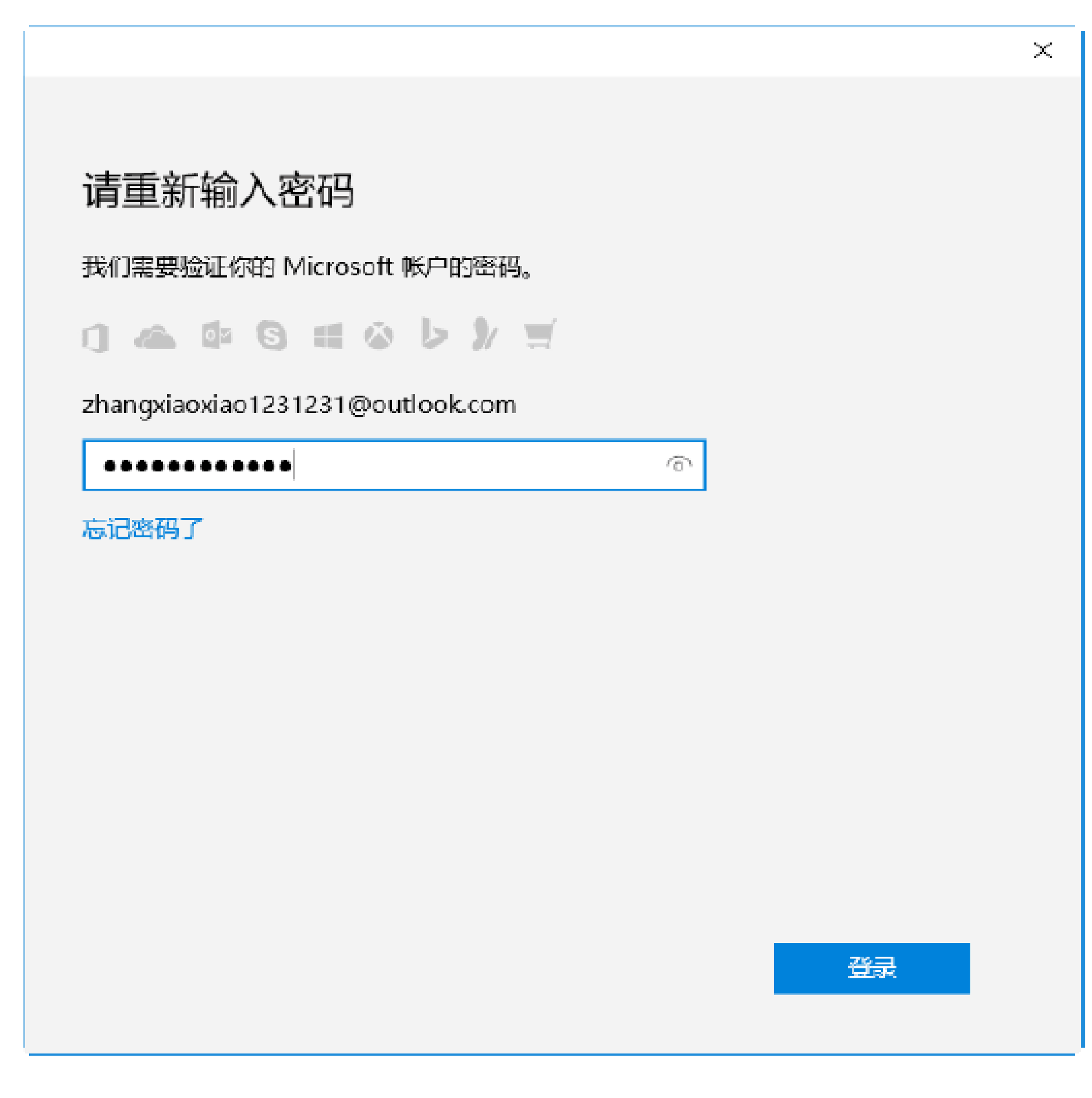
实战8：设置Microsoft账户PIN密码

PIN码是可以替代登录密码的一组数据，当用户登录到Windows及其应用和服务时，系统会要求用户输入PIN码，设置PIN码的操作步骤如下。

Step 01 在“设置-账户”窗口中选择“登录选项”项，在右侧可以看到用于设置PIN码的区域，如下图所示。



Step 02 单击PIN区域下方的“添加”按钮，打开“请重新输入密码”对话框，在其中输入账户的登录密码，如下图所示。



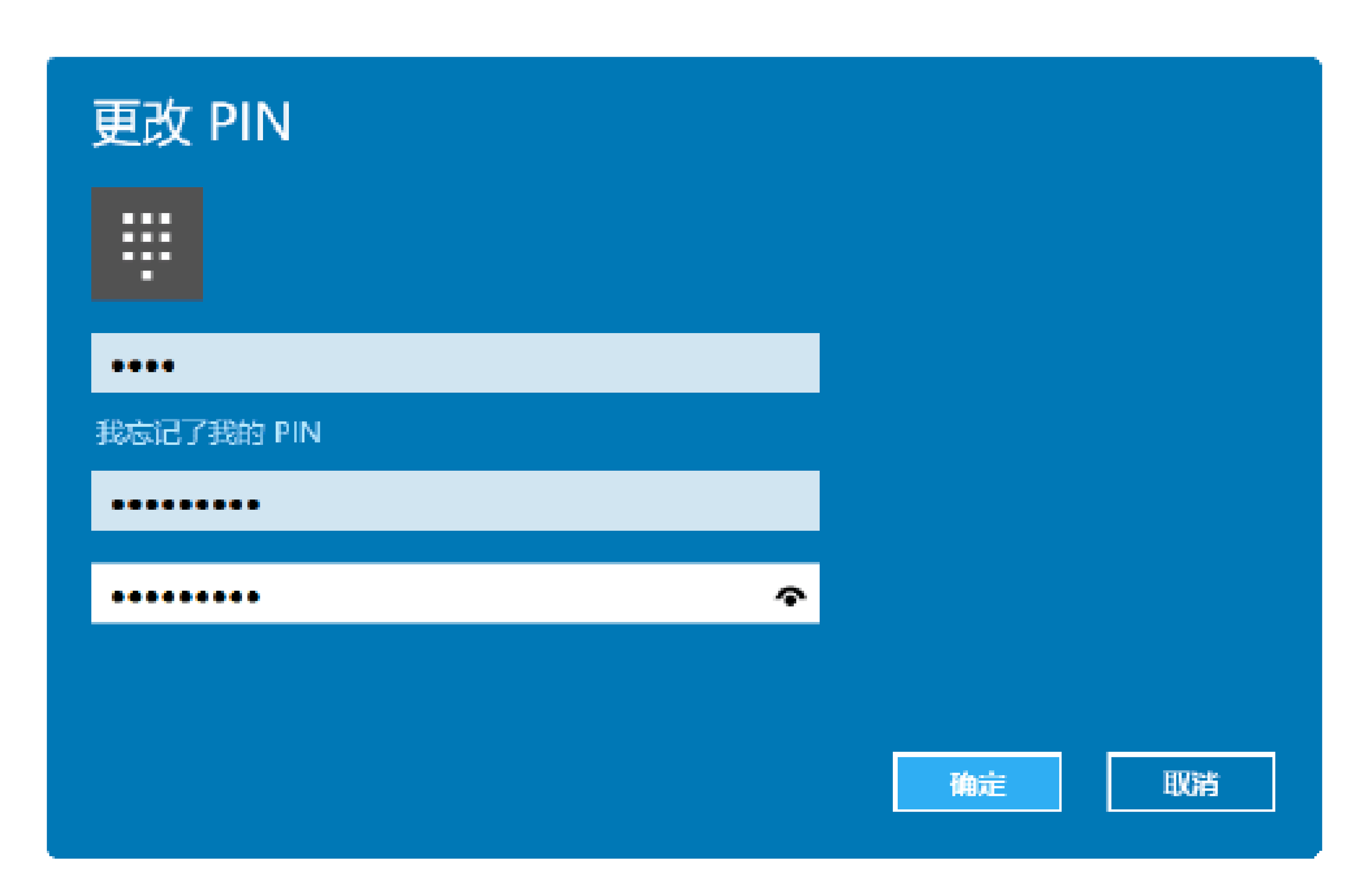
Step 03 单击“登录”按钮，打开“设置PIN”对话框，在其中输入PIN码，如下图所示。



Step 04 单击“确定”按钮，即可完成PIN码的添加操作，并返回到“登录选项”设置界面，如下图所示。



Step 05 如果想要更改PIN码，则可以单击PIN区域下方的“更改”按钮，打开“更改PIN”对话框，在其中输入更改后的PIN码，然后单击“确定”按钮即可，如下图所示。



Step 06 如果忘记了PIN码，则可以在“登录选项”设置界面中单击PIN区域下方的“我忘记了我的PIN”超链接，如下图所示。

Step 07 打开“首先，请验证你的账户密码。”对话框，在其中输入登录账户密码，如下图所示。

Step 08 单击“确定”按钮，打开“设置PIN”对话框，在其中重新输入PIN码，最后单击“确定”按钮即可，如下图所示。



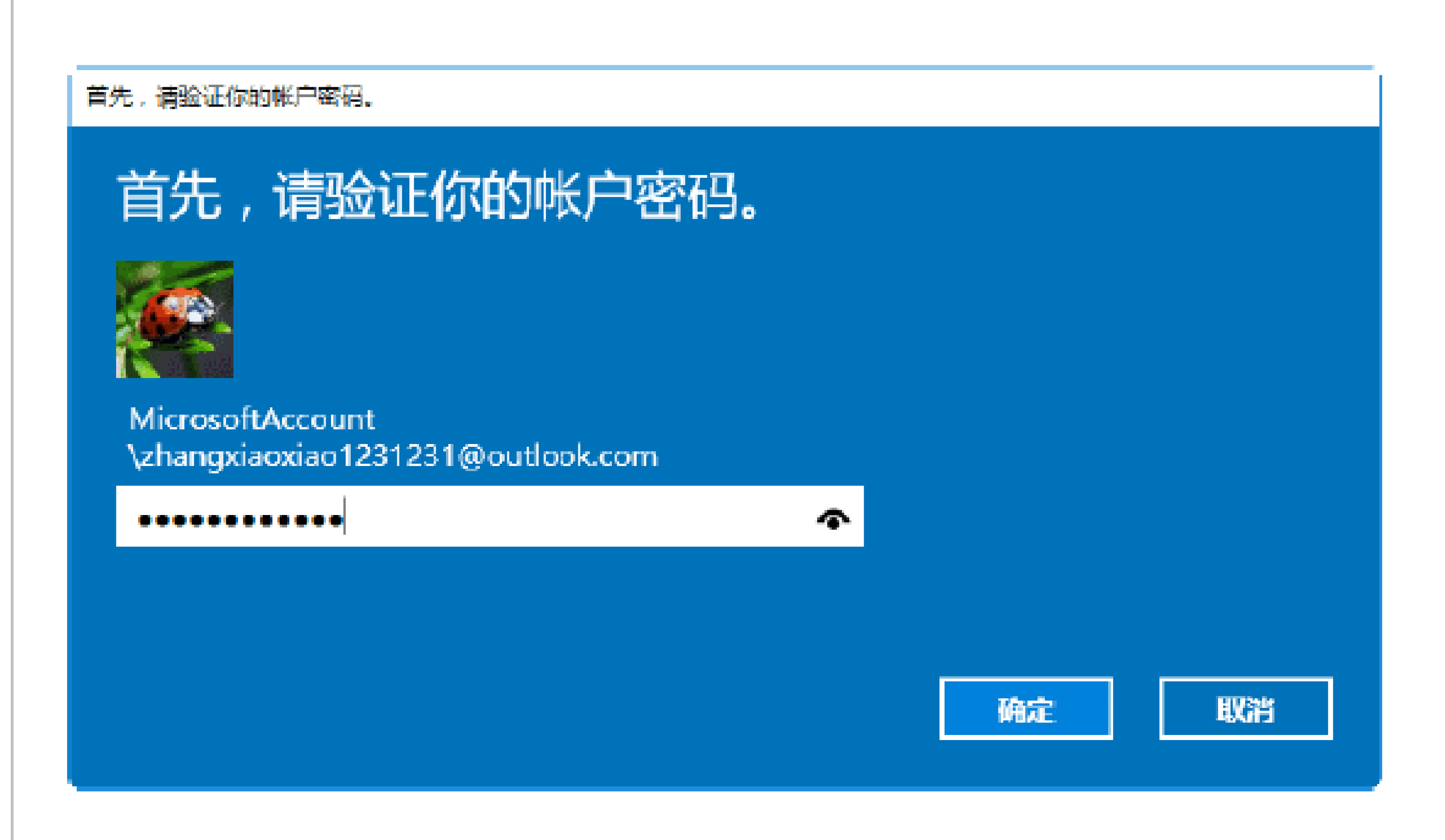
Step 09 如果想要删除PIN码，则可以在“登录选项”设置界面中单击PIN设置区域下方的“删除”按钮，如下图所示。



Step 10 随即在PIN码区域显示出确实要删除PIN码的信息提示，如下图所示。



Step 11 单击“删除”按钮，打开“首先，请验证你的账户密码。”对话框，在其中输入登录密码，如下图所示。



Step 12 单击“确定”按钮，即可删除PIN码，并返回到“登录选项”设置界面，可以看到PIN设置区域只剩下“添加”按钮，说明删除成功，如下图所示。



实战9：设置Microsoft账户图片密码

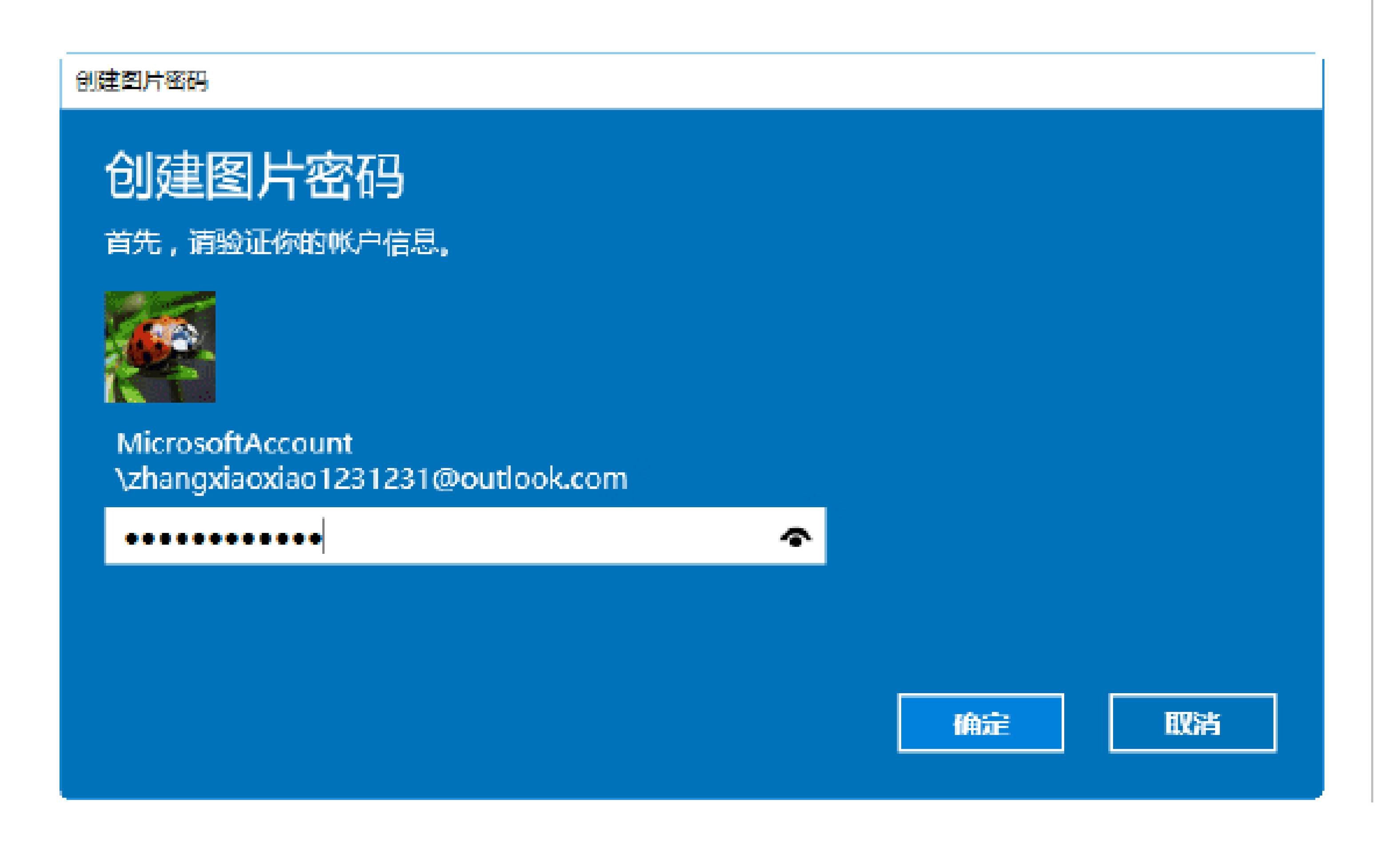
图片密码是一种帮助用户保护触屏计算机的全新方法。要想使用图片密码，用户需要选择图片并在图片上画出各种手势，以此来创建独一无二的图片密码。

创建图片密码的操作步骤如下。

Step 01 在“登录选项”工作界面中单击“图片密码”下方的“添加”按钮，如下图所示。



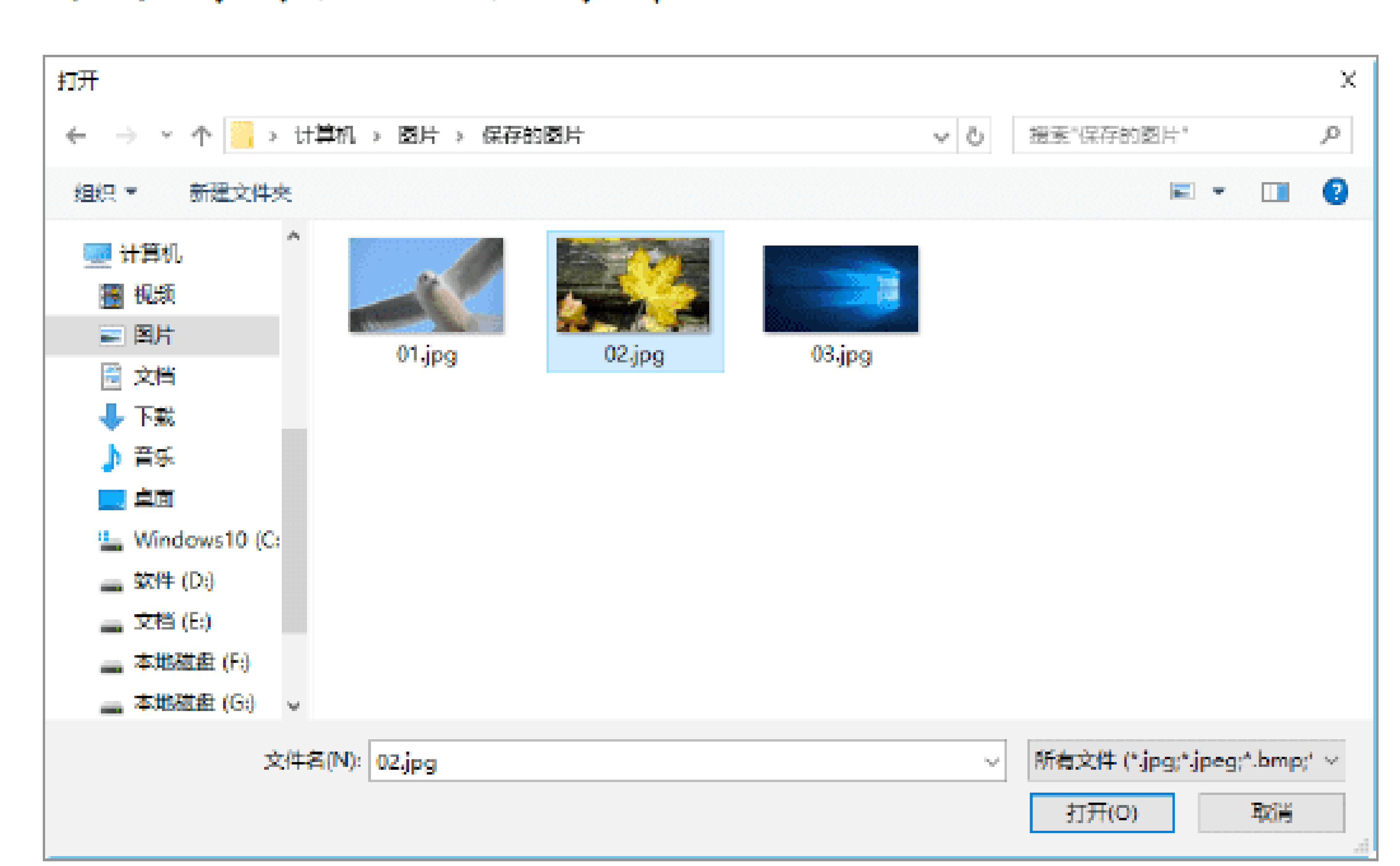
Step 02 打开“创建图片密码”对话框，在其中输入账户登录密码，如下图所示。



Step 03 单击“确定”按钮，进入“图片密码”窗口，如下图所示。



Step 04 单击“选择图片”按钮，打开“打开”对话框，在其中选择用于创建图片密码的图片，如下图所示。



Step 05 单击“打开”按钮，返回到“图片密码”窗口，在其中可以看到添加的图片，如下图所示。



Step 06 单击“使用此图片”按钮，进入“设置你的手势”窗口，在其中通过拖拉鼠标绘制手势，如下图所示。





Step 07 手势绘制完毕后，进入“确认你的手势”窗口，在其中确认上一步绘制的手势，如下图所示。



Step 08 手势确认完毕，进入“恭喜！”窗口，提示用户图片密码创建完成，如下图所示。



Step 09 单击“完成”按钮，返回到“登录选项”工作界面，“添加”按钮已经不存在，说明图片密码添加完成，如下图所示。

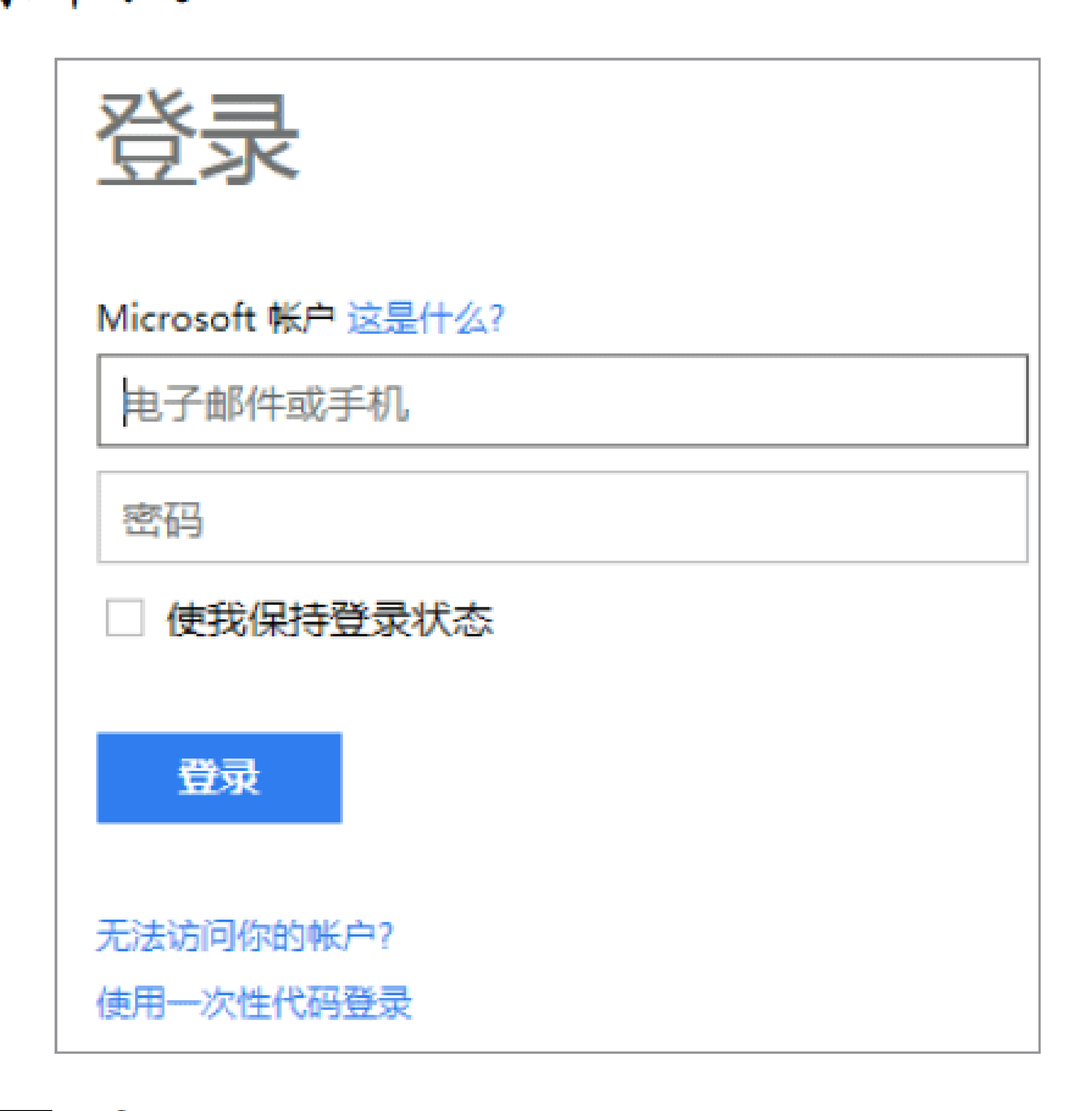


提示：如果想要更改图片密码，可以通过单击“更改”按钮来操作；如果想要删除图片密码，单击“删除”按钮即可。

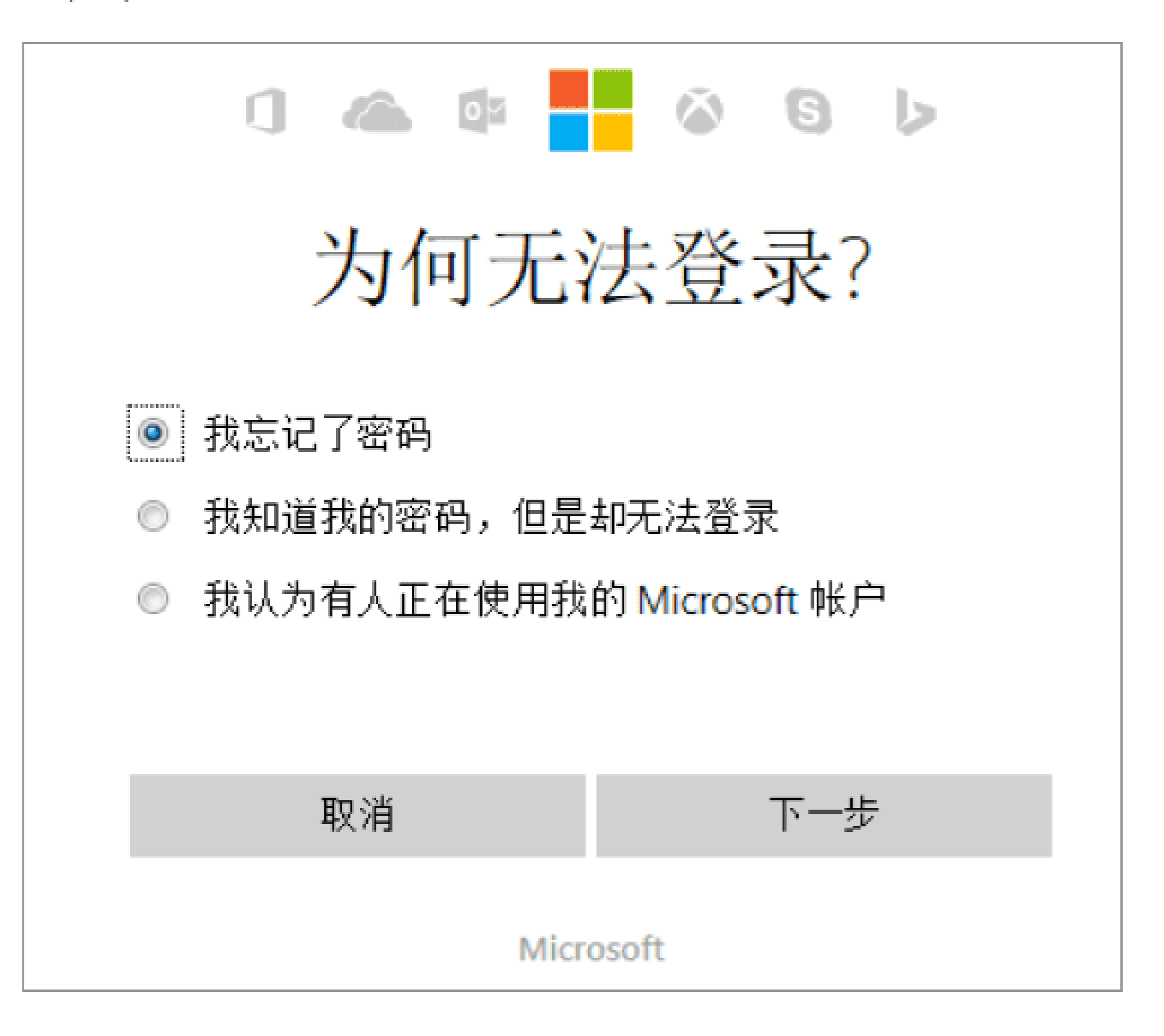
实战10：重置Microsoft账户登录密码

在计算机的使用过程中，忘记计算机开机登录密码是常见的，而Windows 10系统的登录密码是无法强行破解的，需要登录微软的一个找回密码的网站，重置密码，才能登录进入系统桌面，具体的操作步骤如下。

Step 01 打开一台可以上网的计算机，在IE地址栏中输入找回密码网站的网址account.live.com，按Enter键，进入其操作界面，如下图所示。



Step 02 单击“无法访问你的账户？”超链接，打开“为何无法登录？”界面，在其中选中“我忘记了密码”单选按钮，如下图所示。



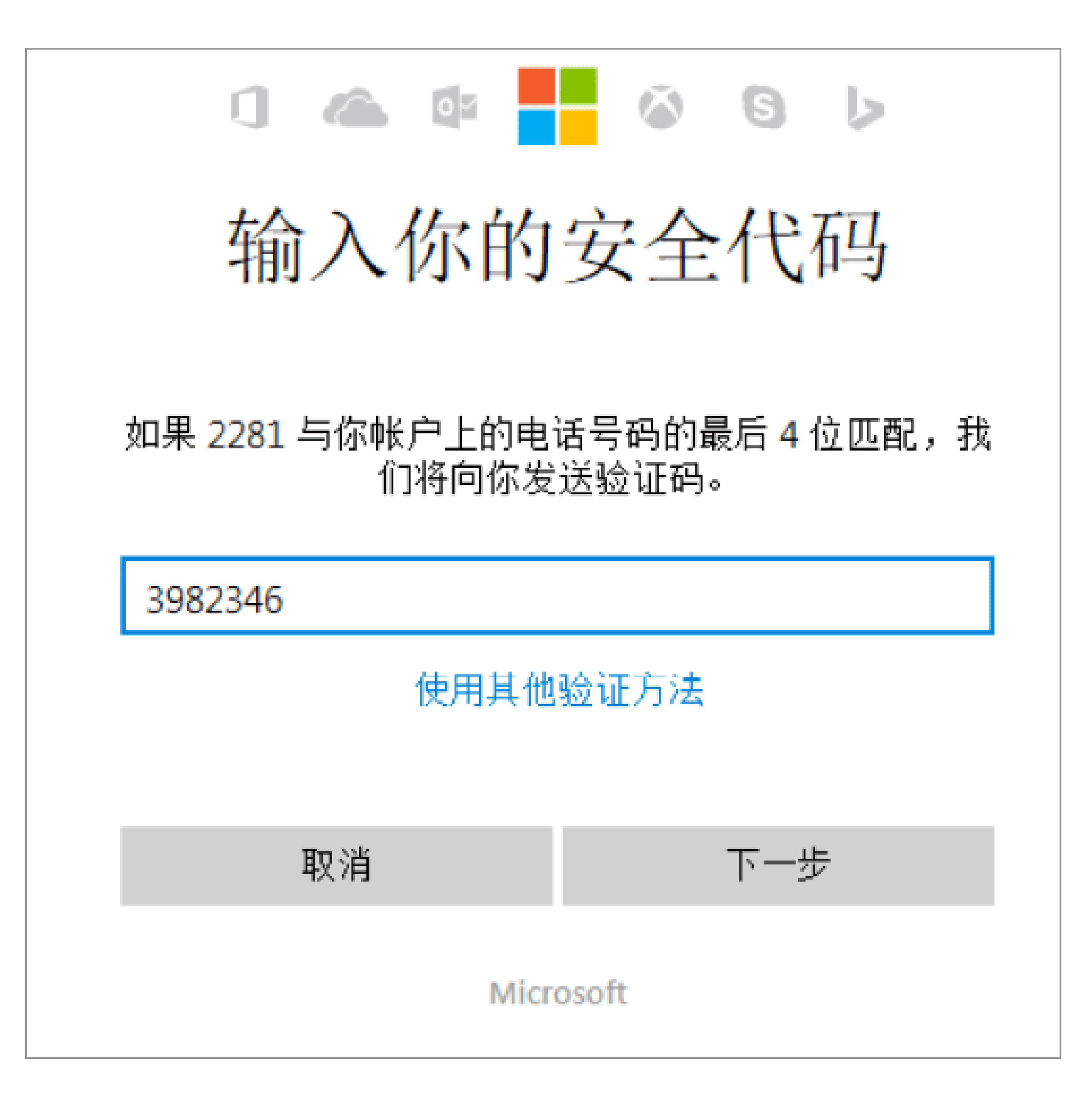
Step 03 单击“下一步”按钮，打开“恢复你的账户”界面，在其中输入要恢复的Microsoft账户和你看到的字符，如下图所示。



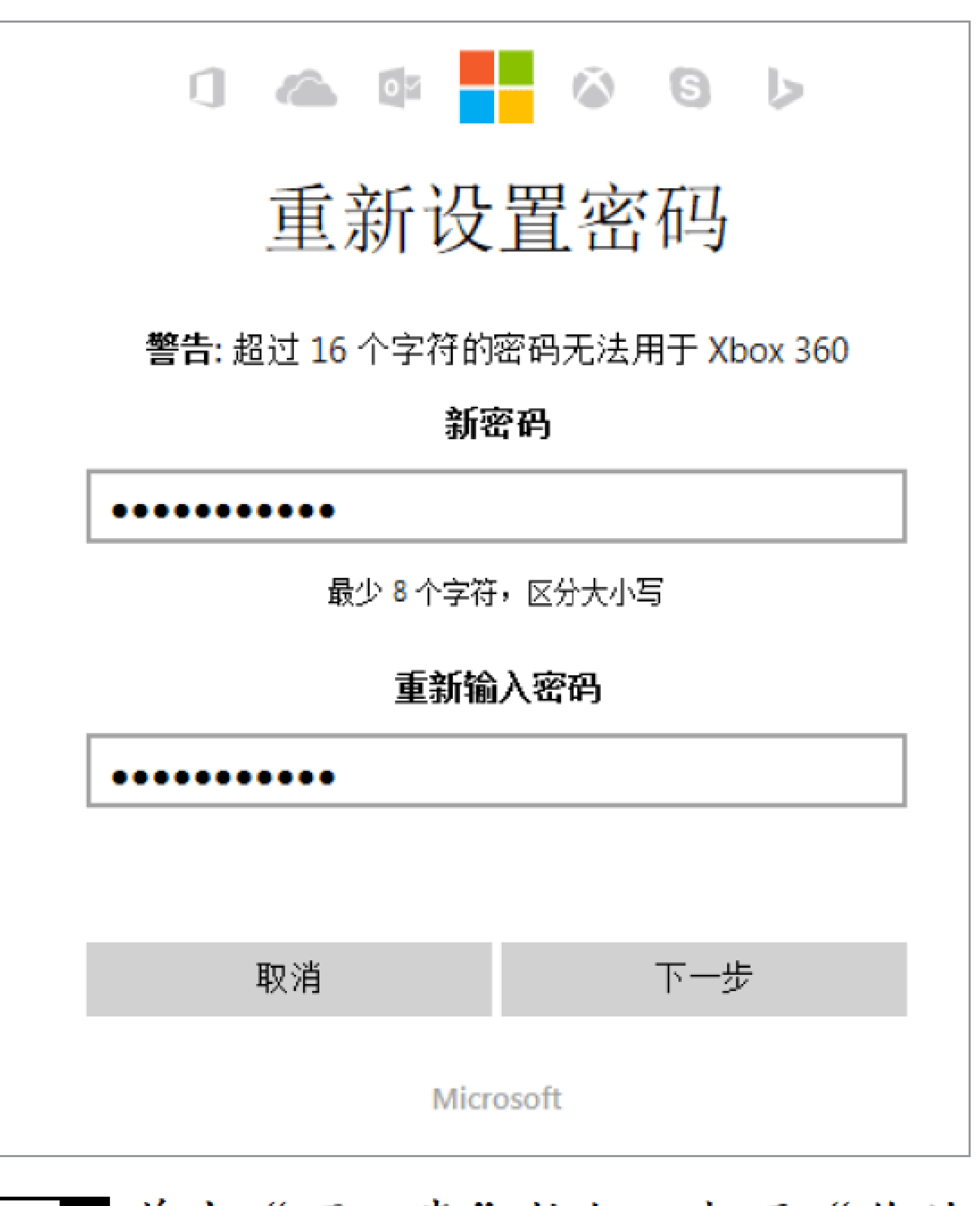
Step 04 单击“下一步”按钮，打开“我们需要验证你的身份”界面，在其中选中“短信至*********81”单选按钮，并在下方的文本框中输入手机号码的后四位，如下图所示。



Step 05 单击“发送代码”按钮，即可向手机中发送安全代码，并打开“输入你的安全代码”界面，在其中输入接收到的安全代码，如下图所示。



Step 06 单击“下一步”按钮，打开“重新设置密码”界面，在其中输入新的密码，并确认再次输入新的密码，如下图所示。



Step 07 单击“下一步”按钮，打开“你的账户已恢复”界面，在其中提示用户可以使用新的安全信息登录到账户，如下图所示。



5.5 实战演练

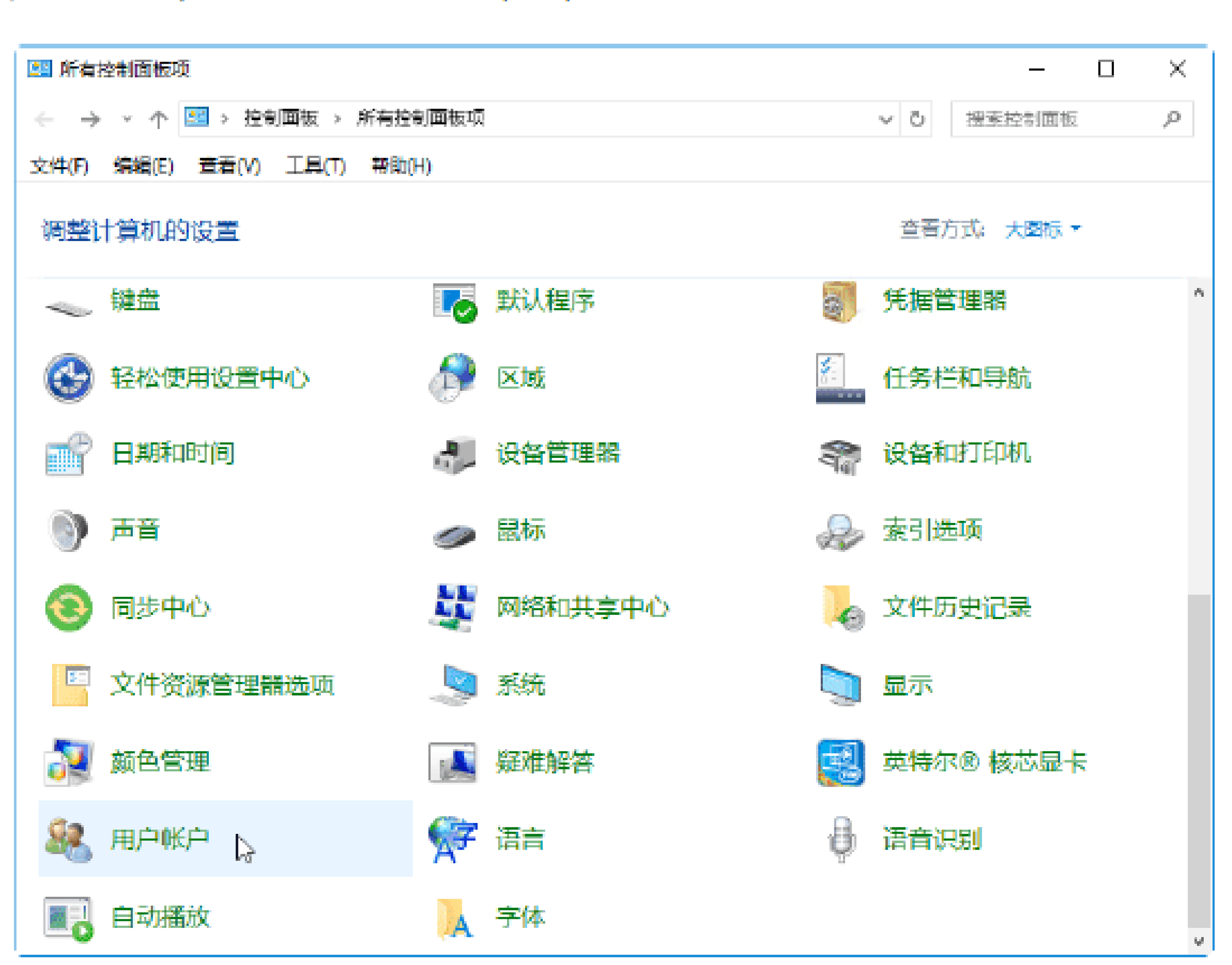


实战演练1——创建用户账户的密码恢复盘

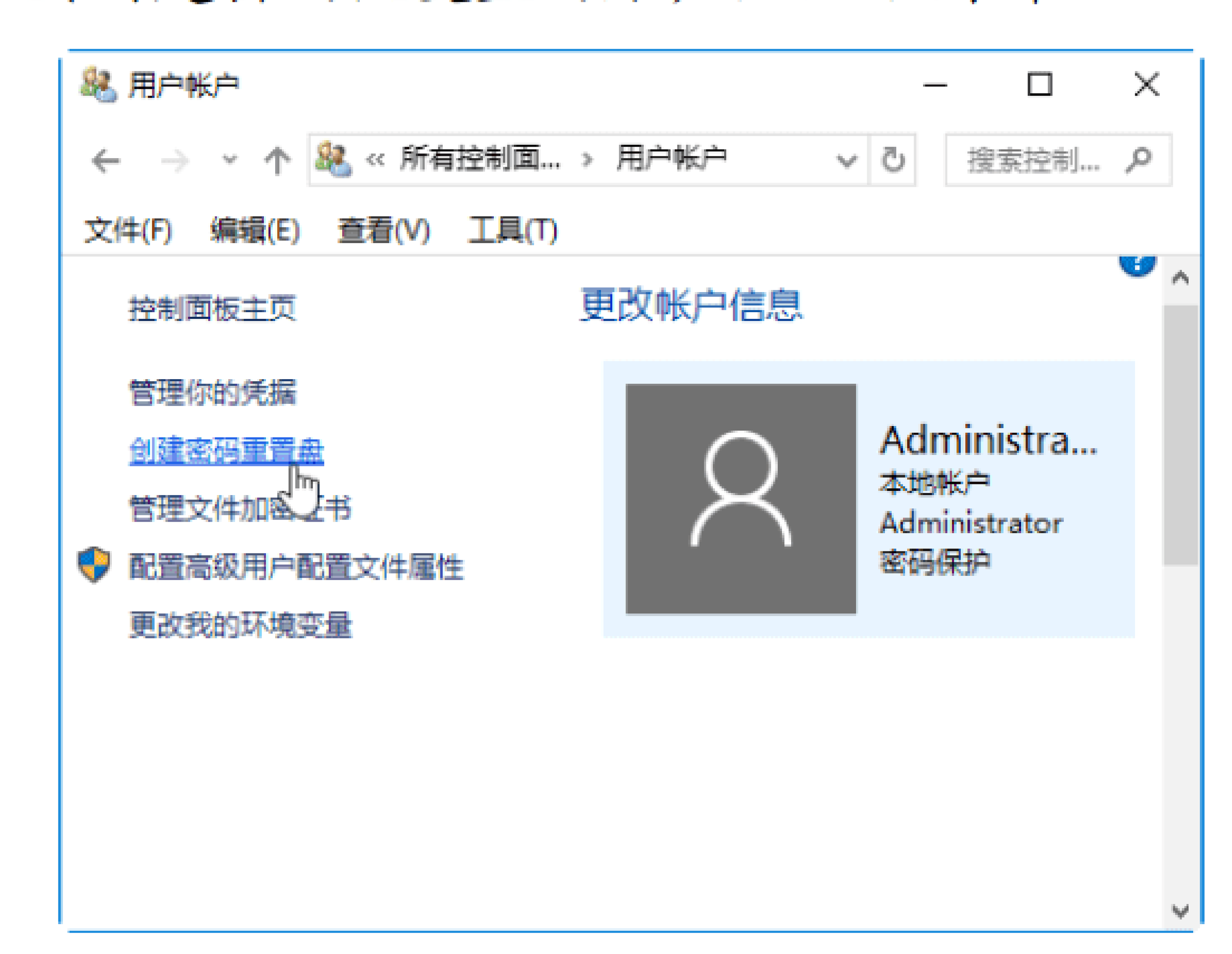
有时，进入系统的账户密码被黑客破解并修改后，用户就进不了系统，但如果事先创建了密码恢复盘，就可以强制进行密码恢复以找到原来的密码。Windows系统自带创建账户密码恢复盘功能，利用该功能可以创建密码恢复盘。

创建密码恢复盘的具体操作步骤如下。

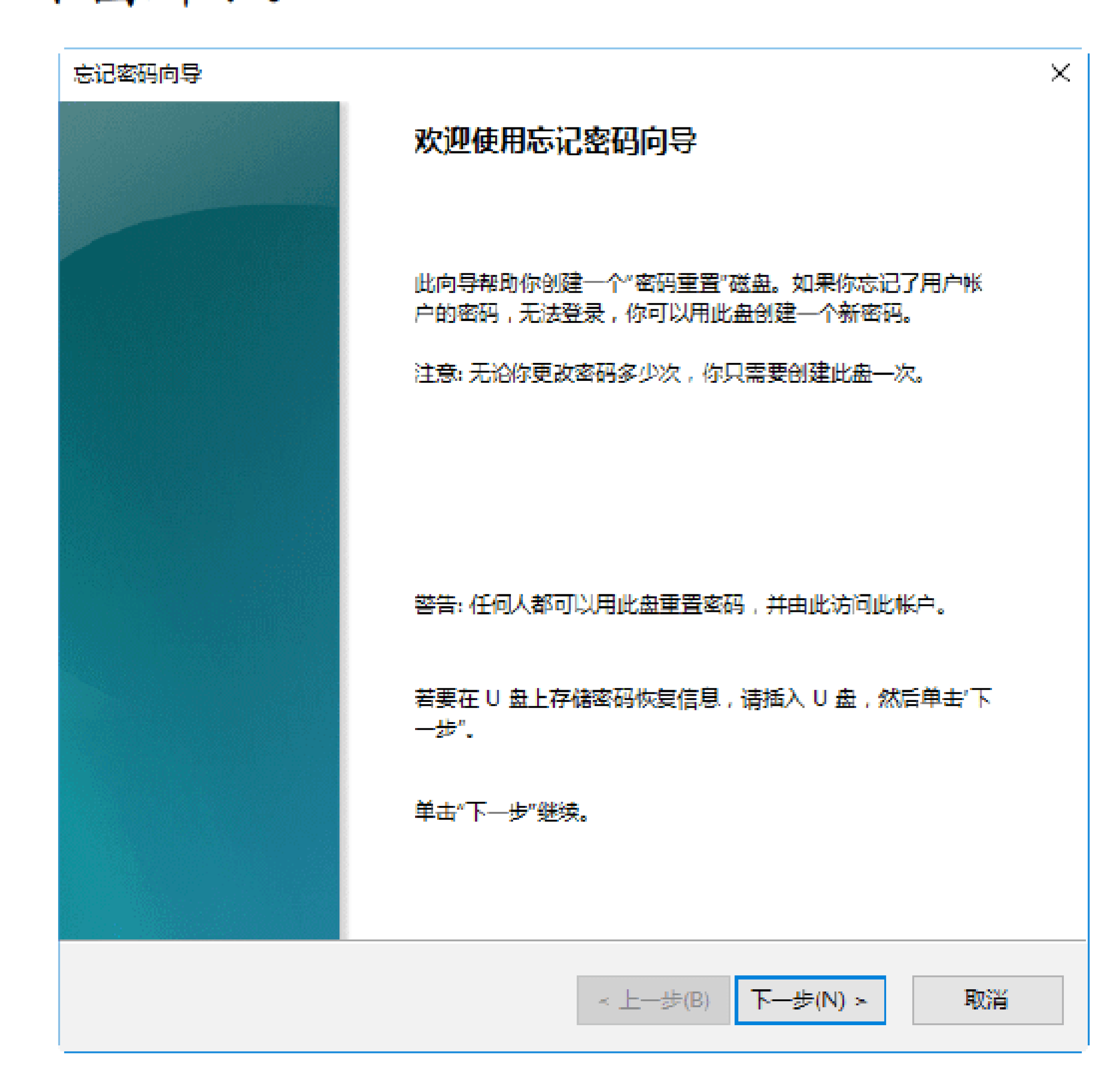
Step 01 选择"开始"→"控制面板"选项，打开"控制面板"窗口，双击"用户账户"图标，如下图所示。



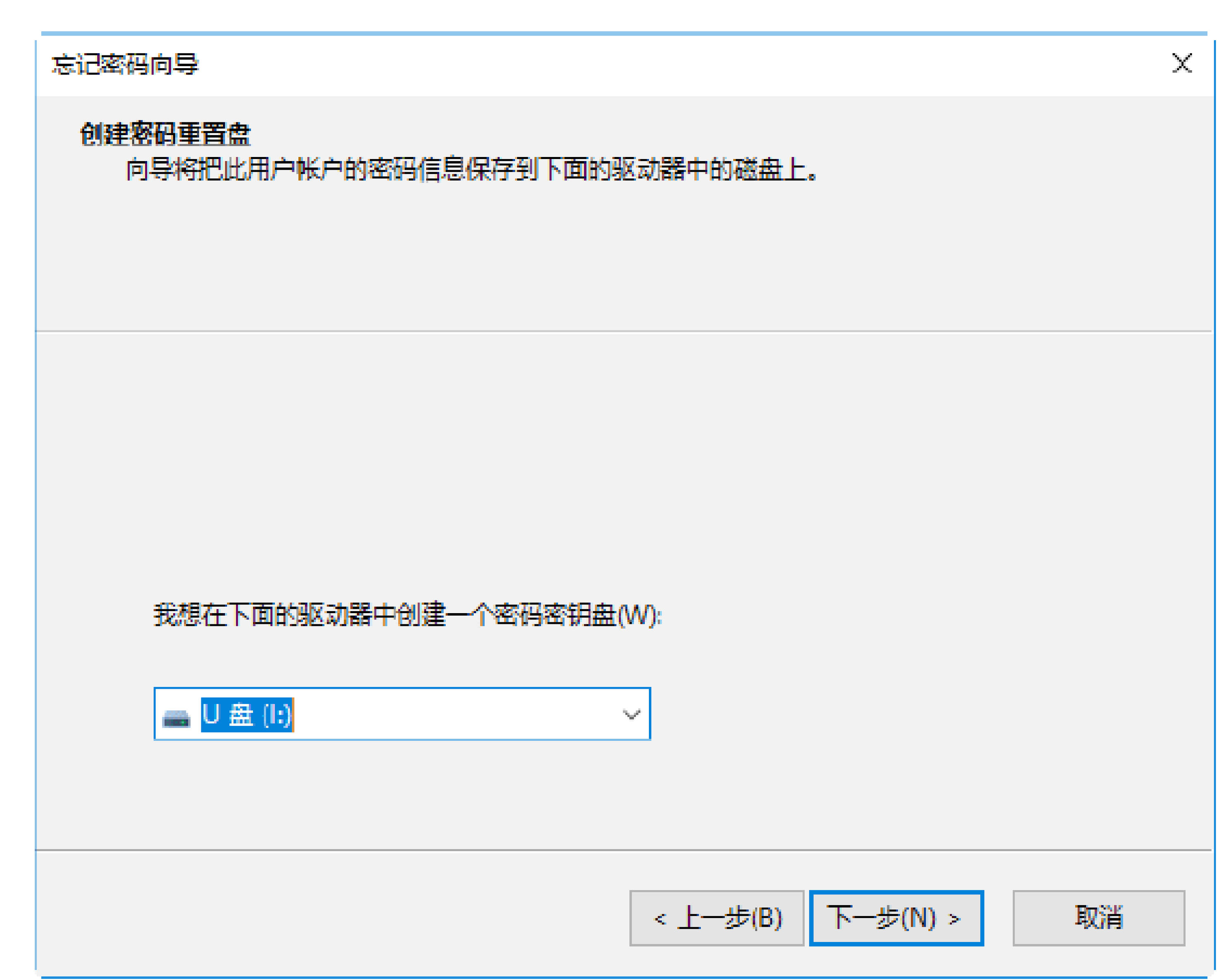
Step 02 打开"用户账户"窗口，在其中选择要创建密码恢复盘的账户，如下图所示。



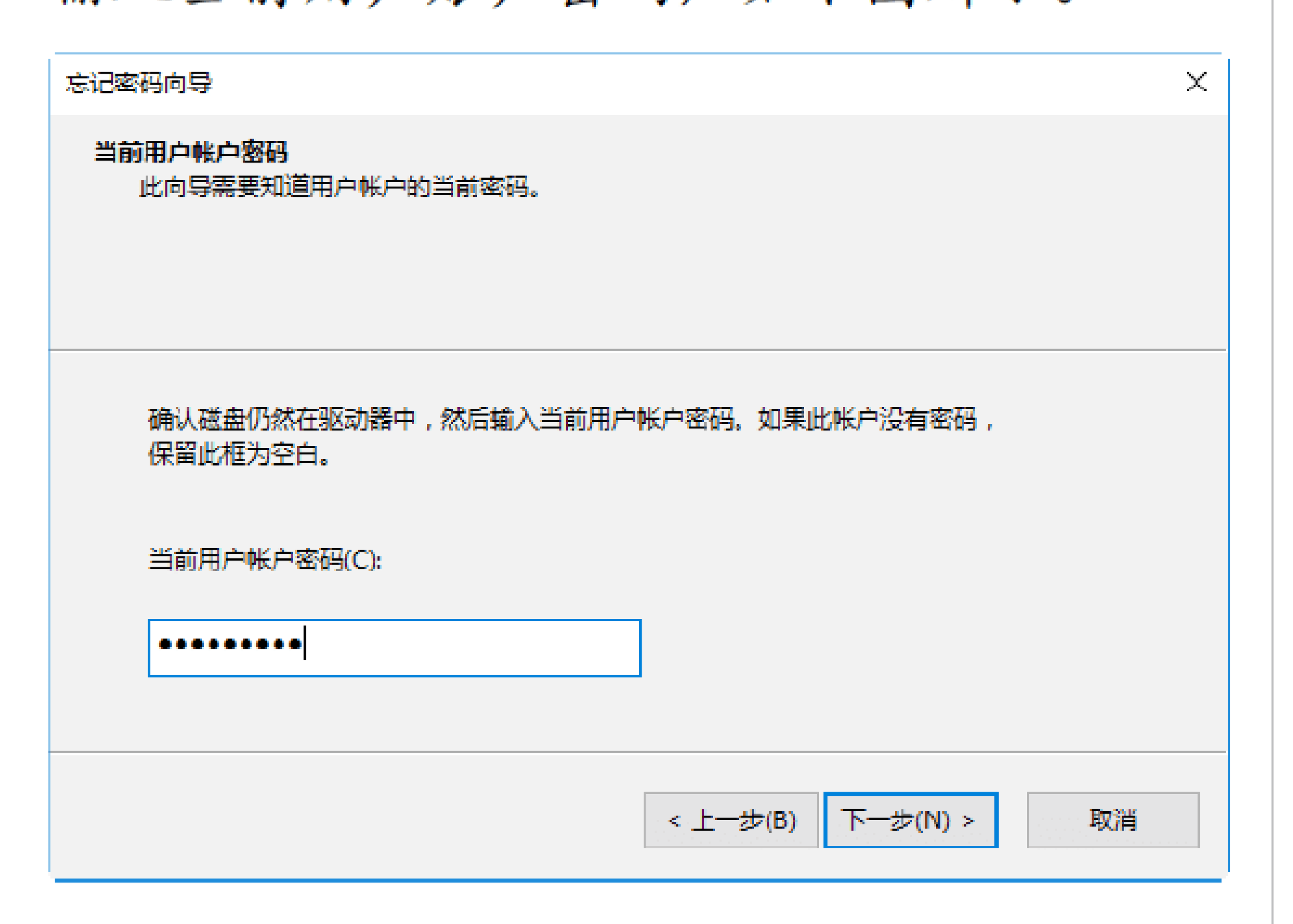
Step 03 单击"创建密码重置盘"超链接，弹出"欢迎使用忘记密码向导"对话框，如下图所示。



Step 04 单击"下一步"按钮，弹出"创建密码重置盘"对话框，如下图所示。



Step 05 单击“下一步”按钮，弹出“当前用户账户密码”对话框，在下面的文本框中输入当前用户账户密码，如下图所示。



Step 06 单击“下一步”按钮，开始创建密码重置盘，创建完毕后，将它保存到安全的地方，这样就可以在密码丢失后进行账户密码恢复了。

实战演练2——本地账户和Microsoft账户的切换

Windows 10操作系统具有两种账户类型，一种是本地账户，一种是Microsoft账户。本地账户和Microsoft账户可以相互切换。

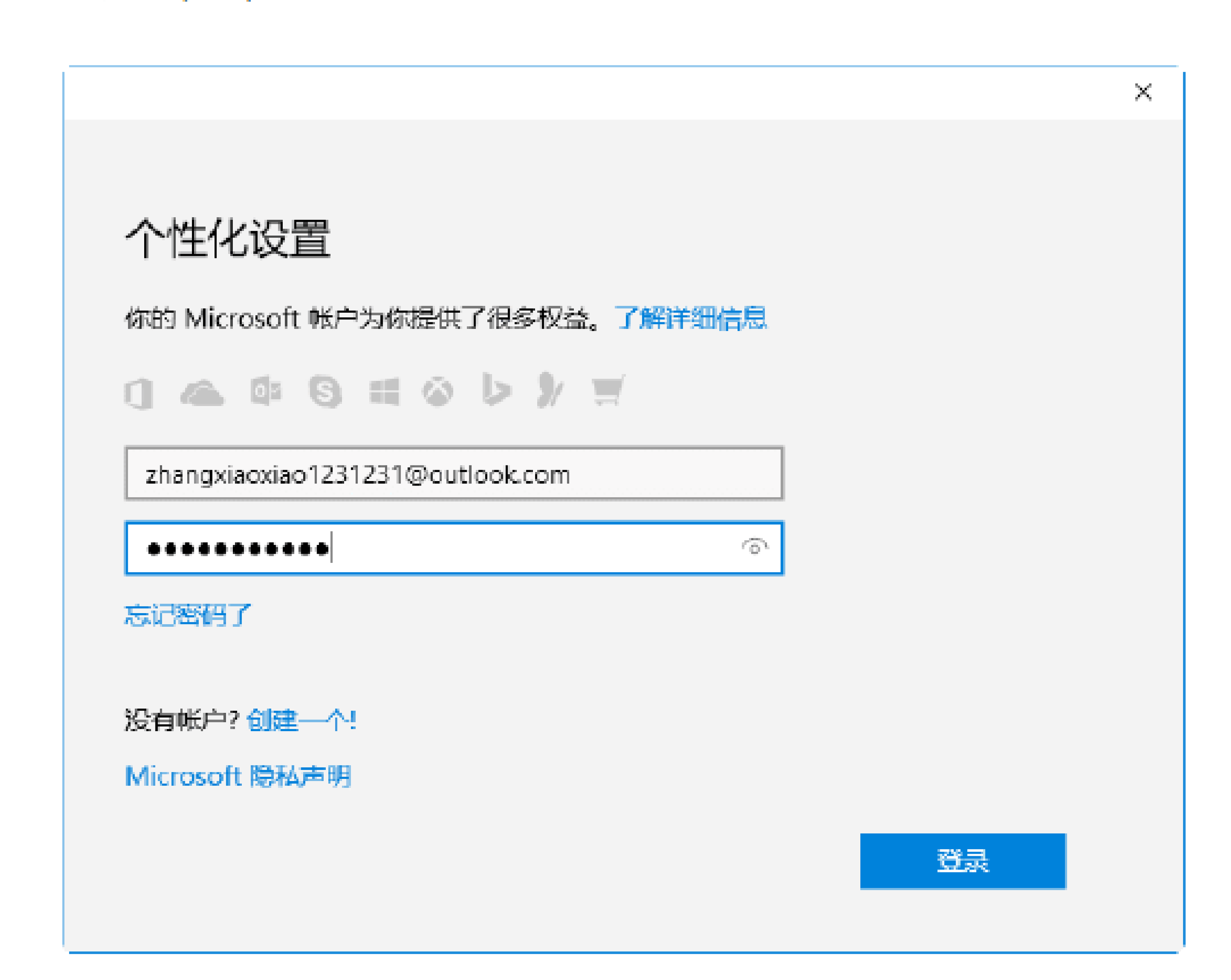
1.本地账户切换到Microsoft账户

将本地账户切换到Microsoft账户可以轻松获取用户所有设备的所有内容，具体的操作步骤如下。

Step 01 在“设置-账户”窗口中选择“你的电子邮件和账户”选项，进入“你的电子邮件和账户”设置界面，如下图所示。

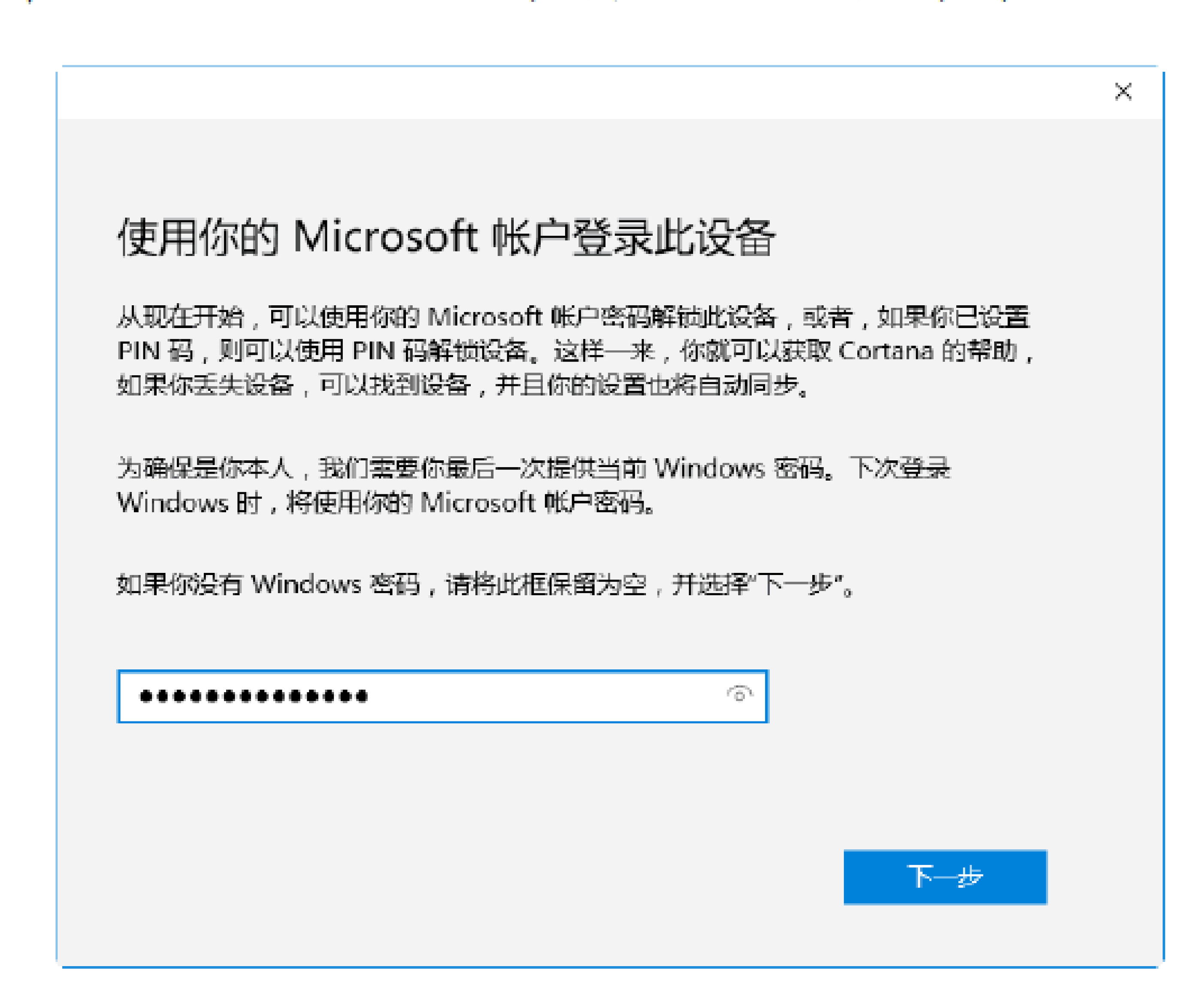


Step 02 单击“改用Microsoft账户登录”超链接，打开“个性化设置”窗口，在其中输入Microsoft账户的电子邮件账户与密码，如下图所示。



Step 03 单击“登录”按钮，打开“使用你的Microsoft账户登录此设备”对话框，在其中输入Windows登录密码，如下图所示。





Step 04 单击“下一步”按钮，即可从本地账户切换到Microsoft账户来登录此设备，如下图所示。



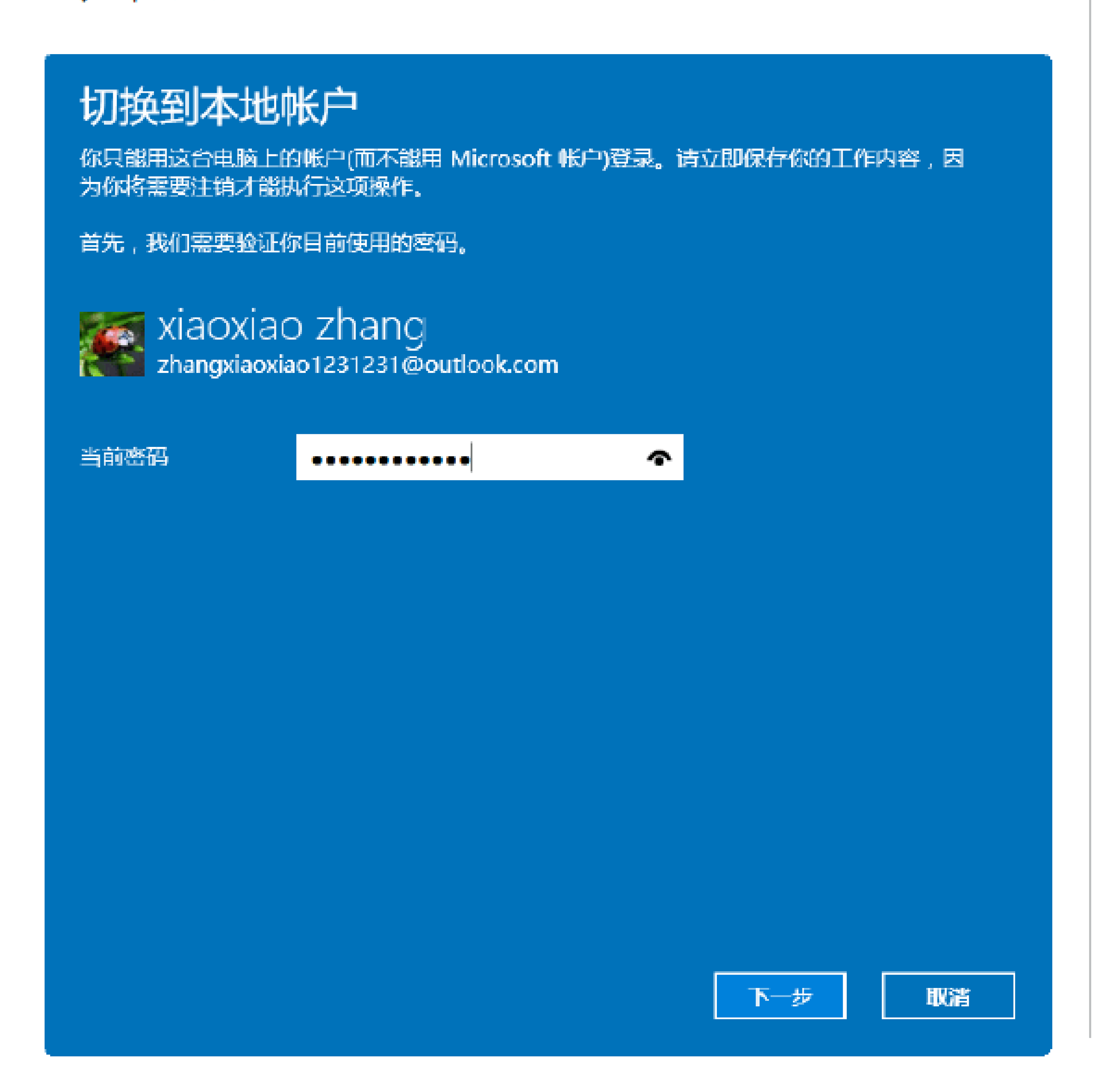
2. Microsoft账户切换到本地账户

本地账户是系统默认的账户，使用本地账户可以轻松管理计算机的本地用户与组，将Microsoft账户切换到本地账户的操作步骤如下。

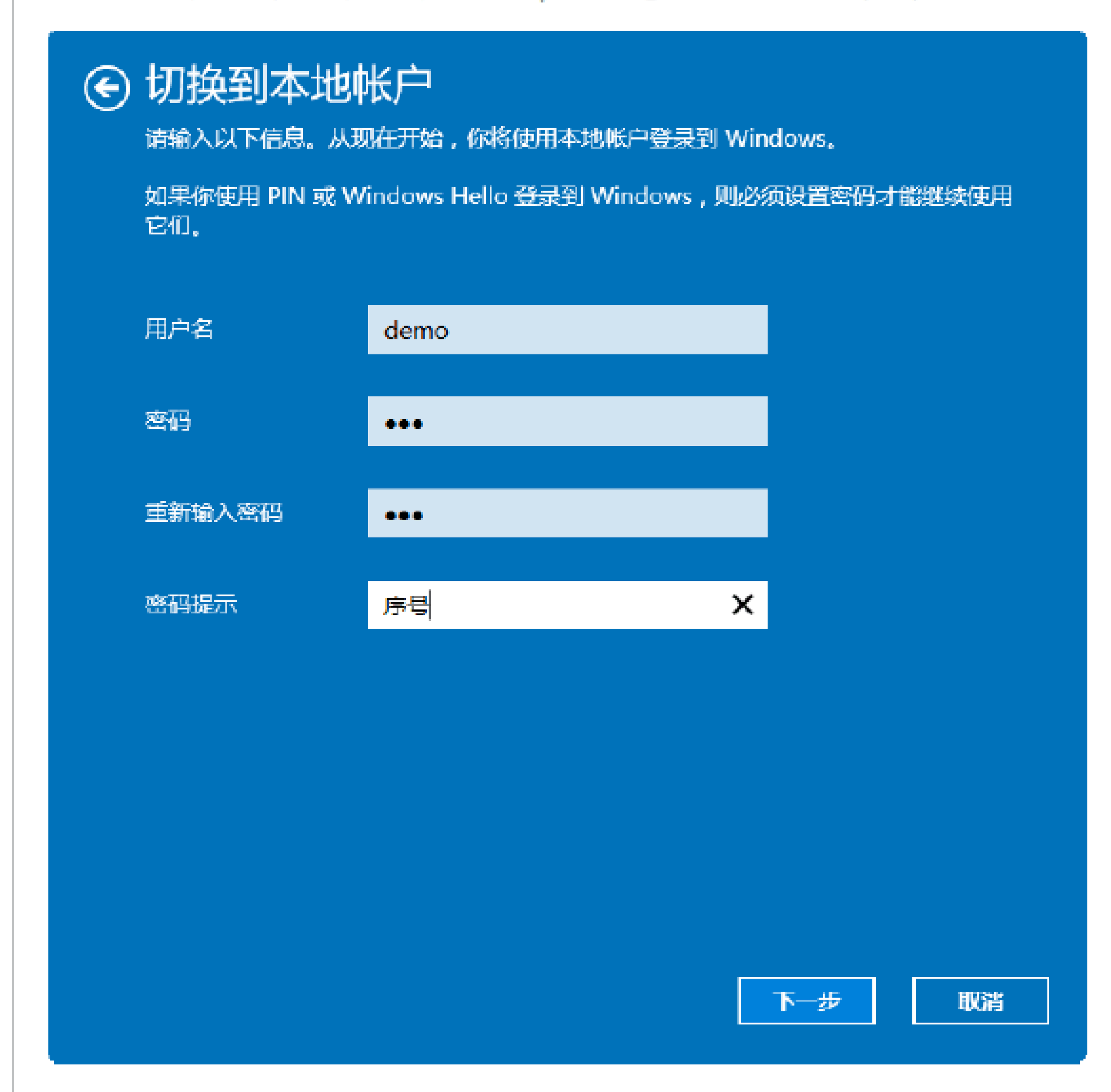
Step 01 以Microsoft账户登录此设备后，选择“设置-账户”窗口中的“你的电子邮件和账户”选项，在打开的设备界面中单击“改用本地账户登录”超链接，如下图所示。



Step 02 打开“切换到本地账户”对话框，在其中输入Microsoft账户的登录密码，如下图所示。



Step 03 单击“下一步”按钮，打开“切换到本地账户”对话框，在其中输入本地账户的用户名、密码和密码提示等信息，如下图所示。



Step 04 单击“下一步”按钮，打开“切换到本地账户”对话框，提示用户所有的操作即将完成，如下图所示。



Step 05 单击“注销并完成”按钮，即可将Microsoft切换到本地账户，如下图所示。



5.6　小试身手

练习1：设置屏幕保护密码

设置屏幕保护密码也是增强计算机安全性的一种方式。设置屏幕保护密码的具体操作步骤如下。

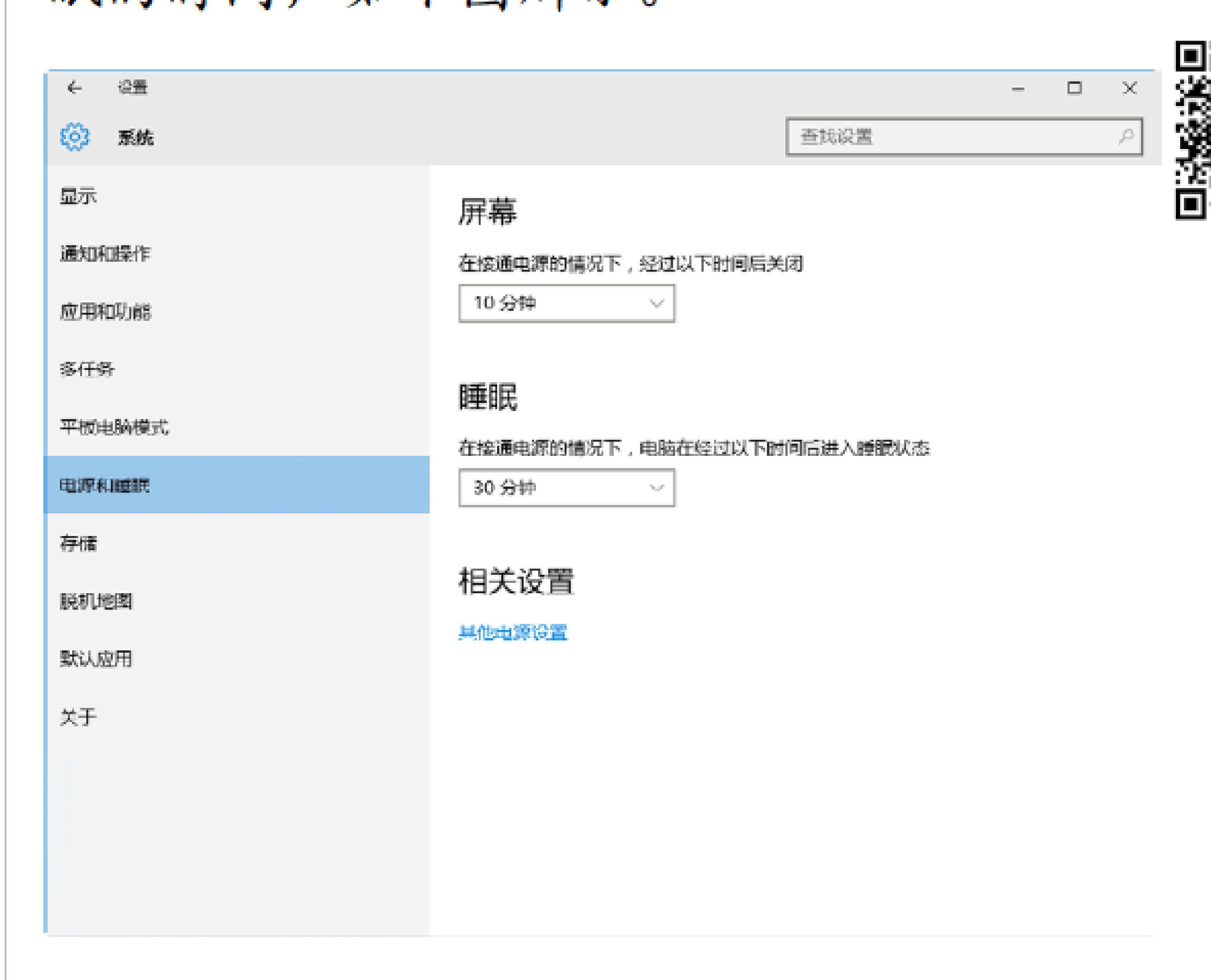
Step 01 在桌面的空白处右击，在弹出的快捷菜单中选择“个性化”选项，如下图所示。



Step 02 打开“个性化”窗口，在其中选择“锁屏界面”选项，如下图所示。



Step 03 在“锁屏界面”设置窗口中单击“屏幕超时设置”超链接，打开“电源和睡眠”设置界面，在其中可以设置屏幕和睡眠的时间，如下图所示。



Step 04 在“锁屏界面”设置窗口中单击“屏幕保护程序设置”超链接，打开“屏幕保护程序设置”对话框，勾选“在恢复时显示登录屏幕”复选框，如下图所示。



Step 05 在“屏幕保护程序”下拉列表中选择系统自带的屏幕保护程序，本实例选择“气泡”选项，此时在上方的预览框中可以看到设置后的效果，如下图所示。





Step 06 在“等待”微调框中设置等待的时间，本实例设置为5分钟，如下图所示。

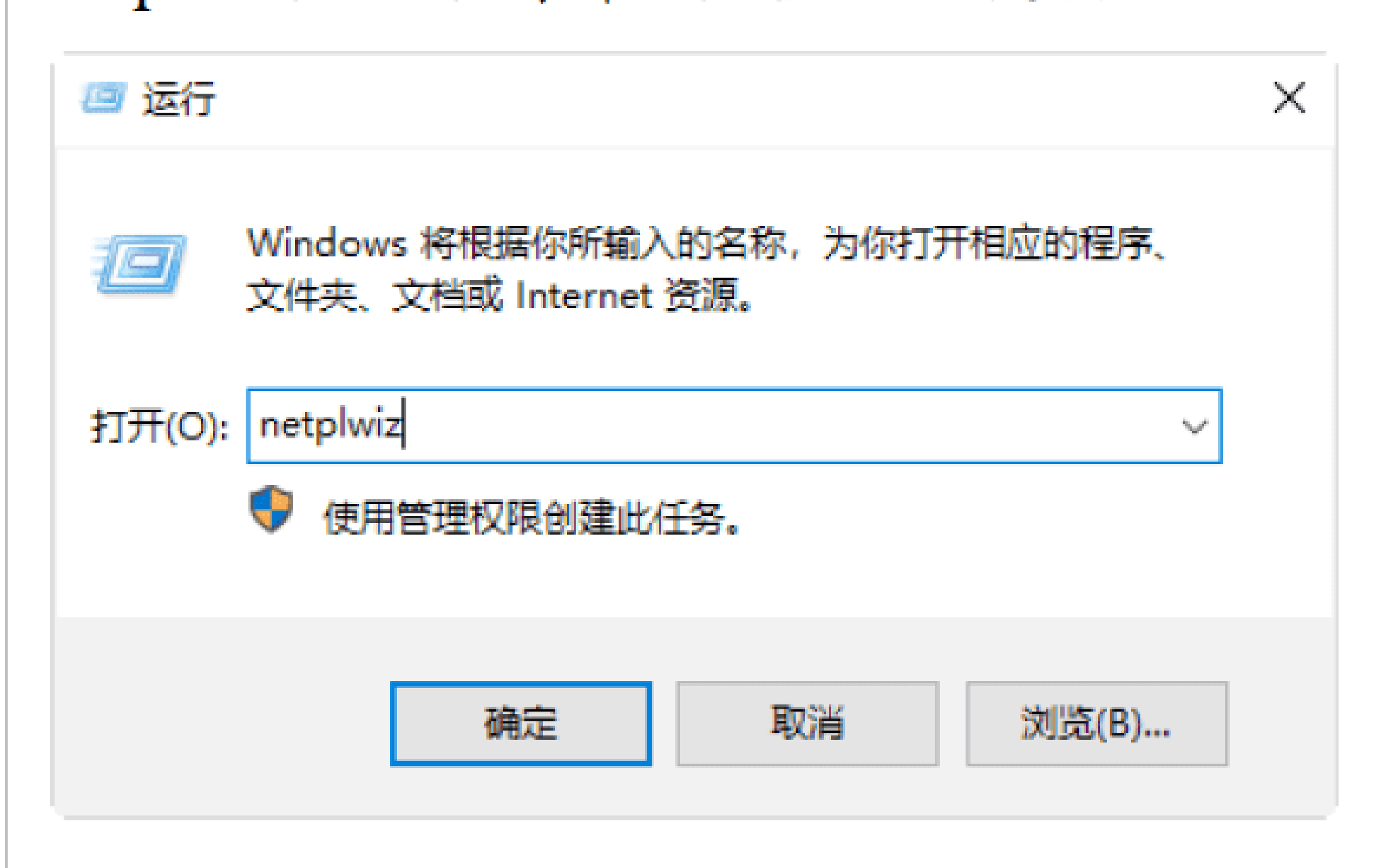


Step 07 设置完成后，单击“确定”按钮，返回到“设置”窗口。这样，如果用户在5分钟内没有对计算机进行任何操作，系统会自动启动屏幕保护程序，用户返回后输入密码即可登录系统。

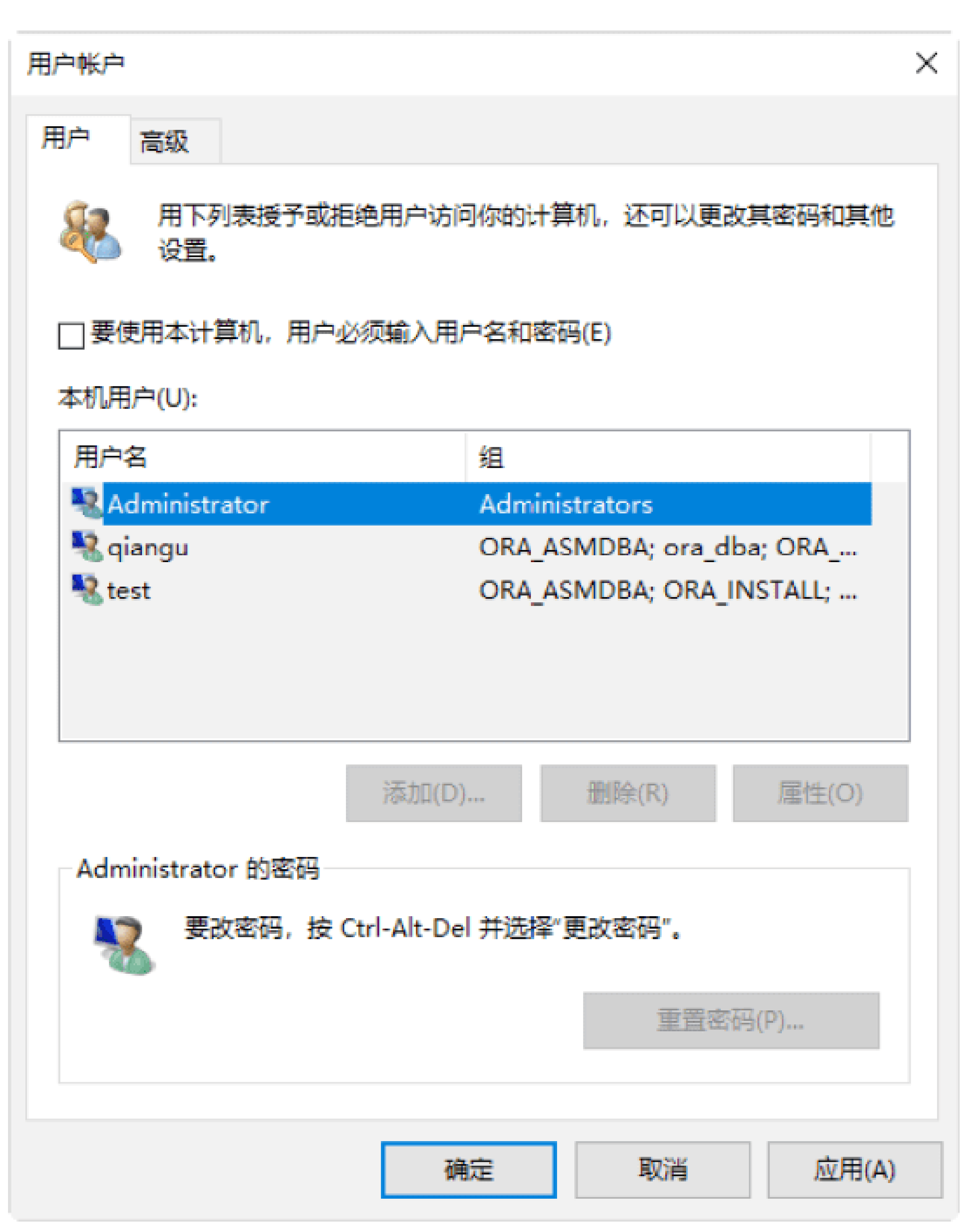
练习2：取消Windows开机密码

虽然使用账户登录密码可以保护计算机的隐私安全，但是每次登录时都要输入密码，对于一部分用户来讲，太过于麻烦。用户可以根据需求，选择是否使用开机密码，如果希望Windows可以跳过输入密码直接登录，可以参照以下步骤。

Step 01 在计算机桌面中，按WIN+R组合键，打开“运行”对话框，在文本框中输入netplwiz，如下图所示，按Enter键确认。

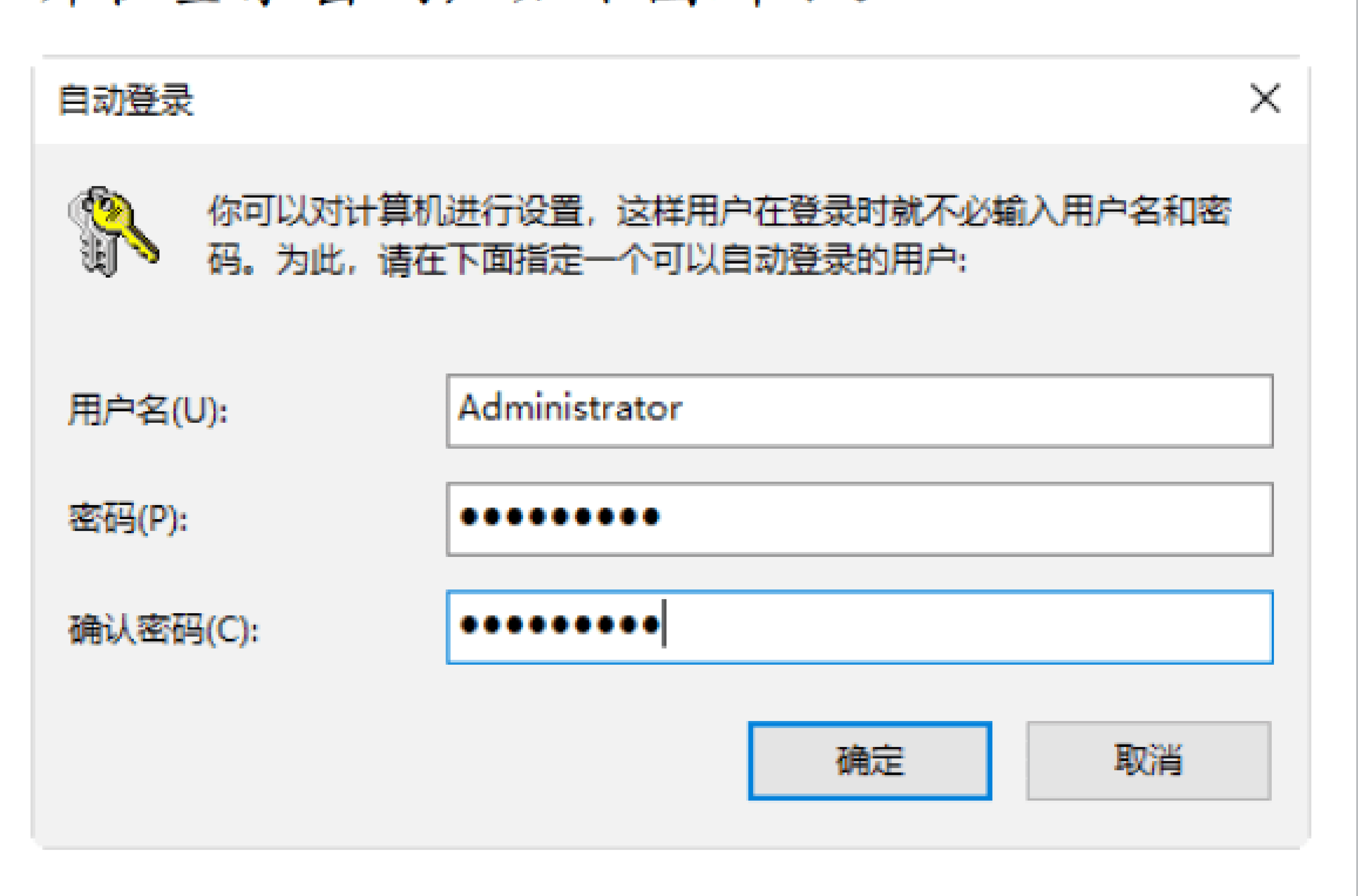


Step 02 弹出“用户账户”对话框，选中本机用户，并取消勾选“要使用本计算机，用户必须输入用户名和密码”复选框，单击“确定”按钮，如下图所示。



Step 03 弹出“自动登录”对话框，在“密

码”和“确认密码”文本框中输入当前账户密码，然后单击“确定”按钮即可取消开机登录密码，如下图所示。



Step 04 再次重新登录时，无须输入用户名和密码，直接登录系统。

第6章　远程控制入侵系统的安全防护

随着计算机的发展以及应用的广泛性，越来越多的操作系统为满足用户的需求，在其中加入了远程控制功能，这一功能本来是方便用户使用的，但也为黑客们所利用。本章介绍系统入侵与远程控制的防护策略，主要内容包括系统入侵的常用手段、远程控制工具入侵系统的方法以及远程控制的防护策略等。

6.1　什么是远程控制

远程控制是在网络上由一台计算机（主控端/客户端）远距离去控制另一台计算机（被控端/服务器端）的技术，而远程一般是指通过网络控制远端计算机，和操作自己的计算机一样。

远程控制一般支持LAN、WAN、拨号、互联网等网络方式。此外，有的远程控制软件还支持通过串口、并口等方式来对远程主机进行控制。随着网络技术的发展，目前很多远程控制软件提供通过Web页面以Java技术来控制远程计算机，这样可以实现不同操作系统下的远程控制。远程控制的应用体现在以下几个方面。

（1）远程办公。这种远程的办公方式不仅大大缓解了城市交通状况，还免去了人们上下班路上奔波的辛劳，更可以提高企业员工的工作效率和工作兴趣。

（2）远程技术支持。一般情况下，远距离的技术支持必须依赖技术人员和用户之间的电话交流来进行，这种交流既耗时又容易出错。有了远程控制技术，技术人员就可以远程控制用户的计算机，就像直接操作本地计算机一样，只需要用户的简单帮助就可以看到该机器存在问题的第一手材料，很快找到问题的所在并加以解决。



（3）远程交流。商业公司可以依靠远程技术与客户进行远程交流。采用交互式的教学模式，通过实际操作来培训用户，从专业人员那里学习知识就变得十分容易。而教师和学生之间也可以利用这种远程控制技术实现教学问题的交流，学生可以直接在计算机中进行习题的演算和求解，在此过程中，教师能够轻松看到学生的解题思路和步骤，并加以实时的指导。

（4）远程维护和管理。网络管理员或者普通用户可以通过远程控制技术对远端计算机进行安装和配置软件、下载并安装软件修补程序、配置应用程序和系统软件设置等操作。

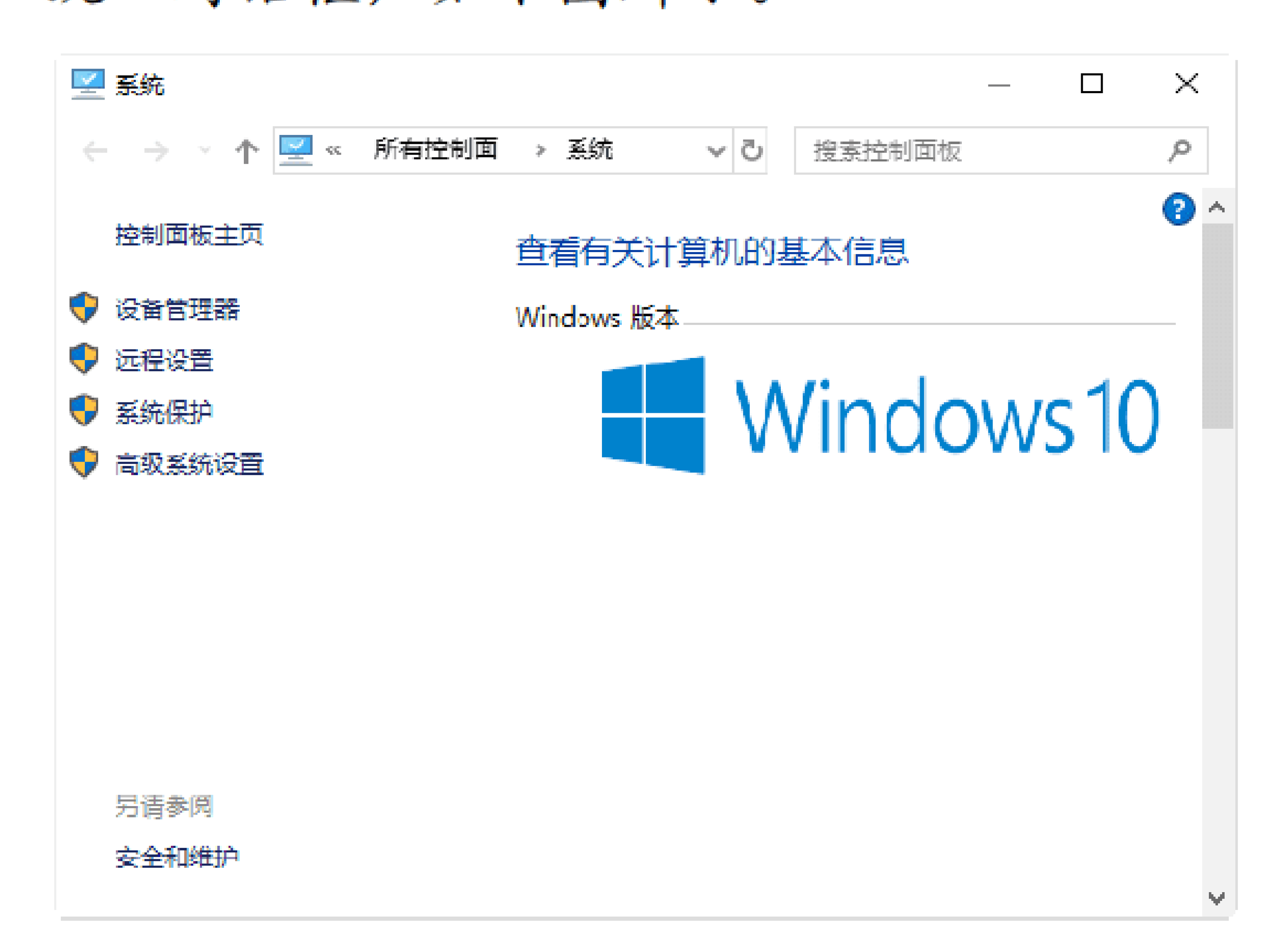
6.2　通过Windows远程桌面入侵系统

通过远程控制工具入侵目标主机系统的方法有多种，最常见的有telnet、ssh、vnc、远程桌面等技术。除此之外，还有一些专门的远程控制工具，如RemotelyAnywhere、PcAnywhere等。

实战1：开启Windows远程桌面功能

远程桌面功能是Windows系统自带的一种远程管理工具，具有操作方便、直观等特征。在Windows系统中开启远程桌面的具体操作步骤如下。

Step 01 右击“此计算机”图标，在弹出的快捷菜单中选择“属性”选项，打开“系统”对话框，如下图所示。



Step 02 选择“远程设置”选项，打开“系统属性”对话框，在其中勾选“允许远程协助连接这台计算机”复选框，设置完毕后，单击“确定”按钮，即可完成设置，如下图所示。



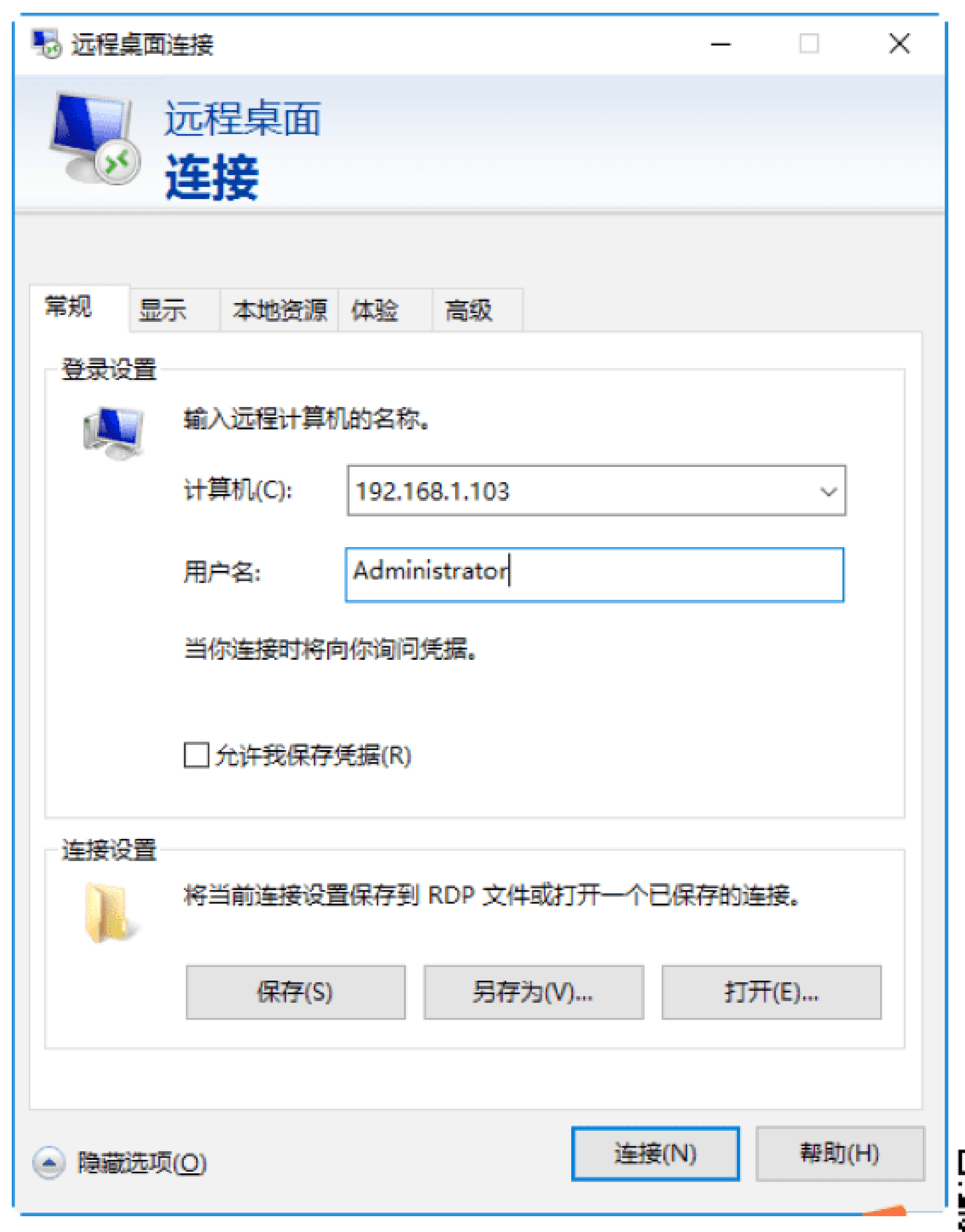
实战2：使用远程桌面功能实现远程控制

如果目标主机开启了远程桌面连接功能，就可以在网络中的其他主机上连接控制这台目标主机了，通过Windows远程桌面实现远程控制的操作步骤如下。

Step 01 选择“开始”→“Windows附件”→“远程桌面连接”选项，打开“远程桌面连接”窗口，如下图所示。



Step 02 单击“显示选项”按钮，展开即可看到选项的具体内容。在“常规”选项卡中的“计算机”下拉文本框中选择需要远程连接的计算机名称或IP地址；在“用户名”文本框中输入相应的用户名，如下图所示。

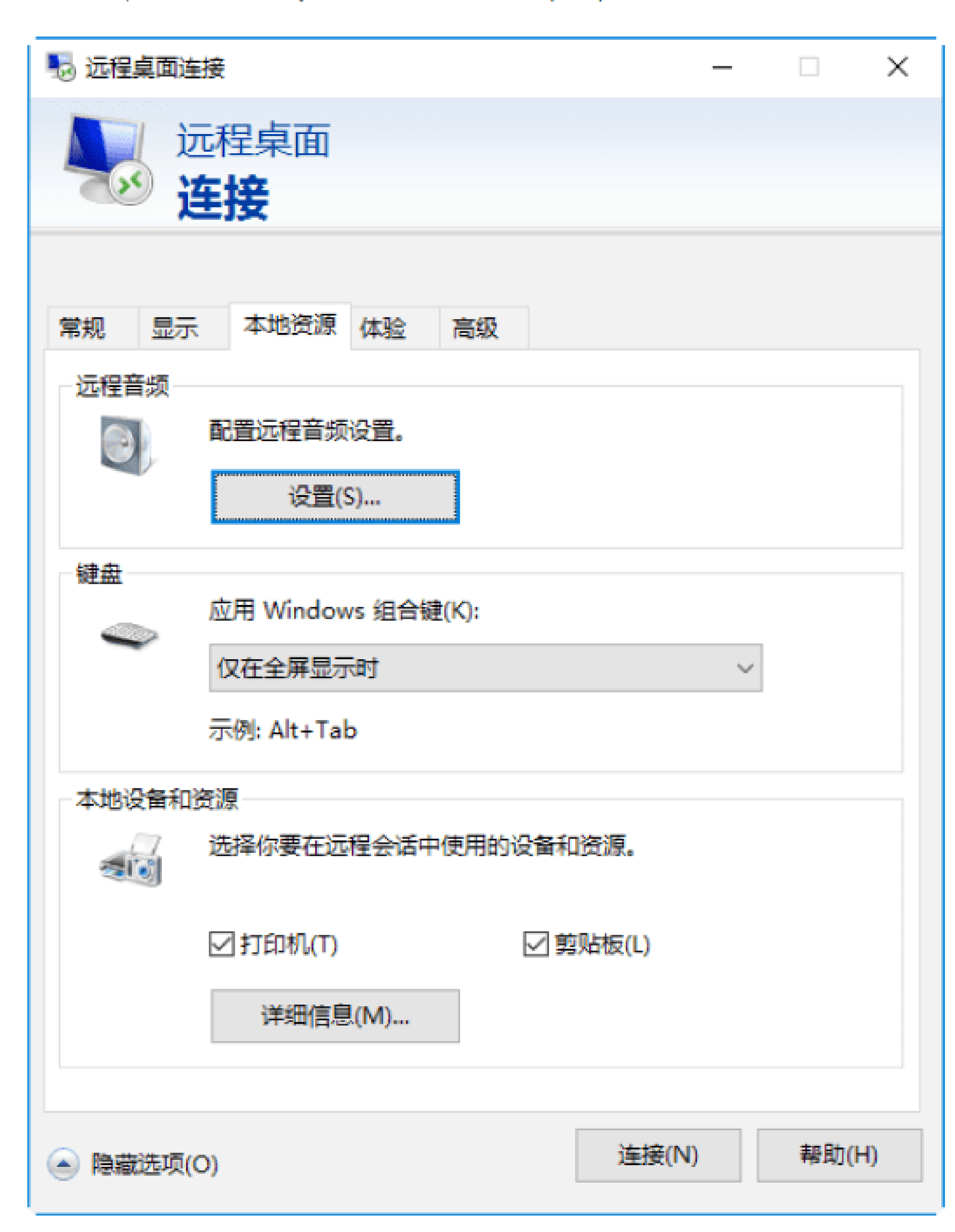




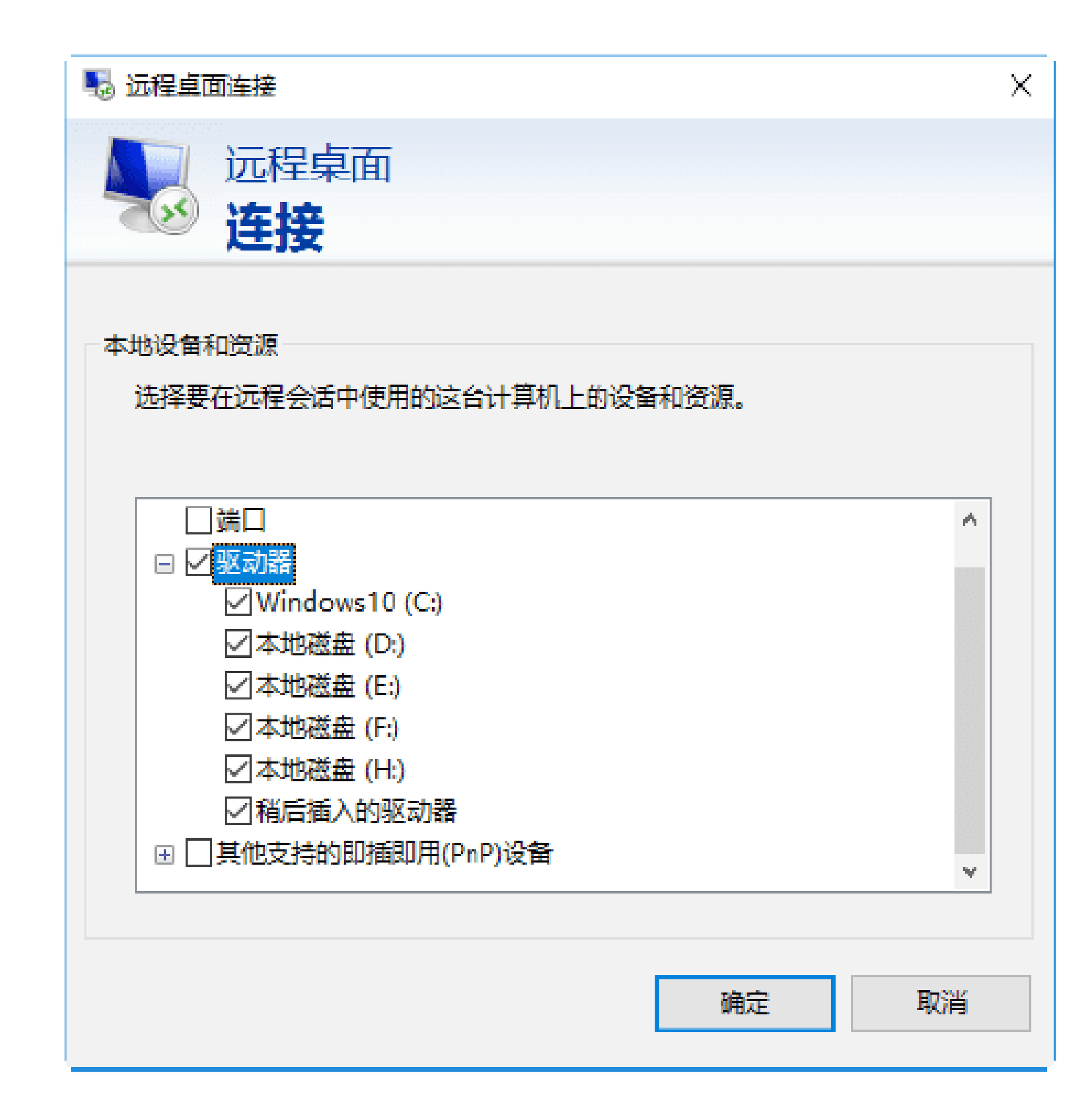
Step 03 选择“显示”选项卡，在其中可以设置远程桌面的大小、颜色等属性，如下图所示。



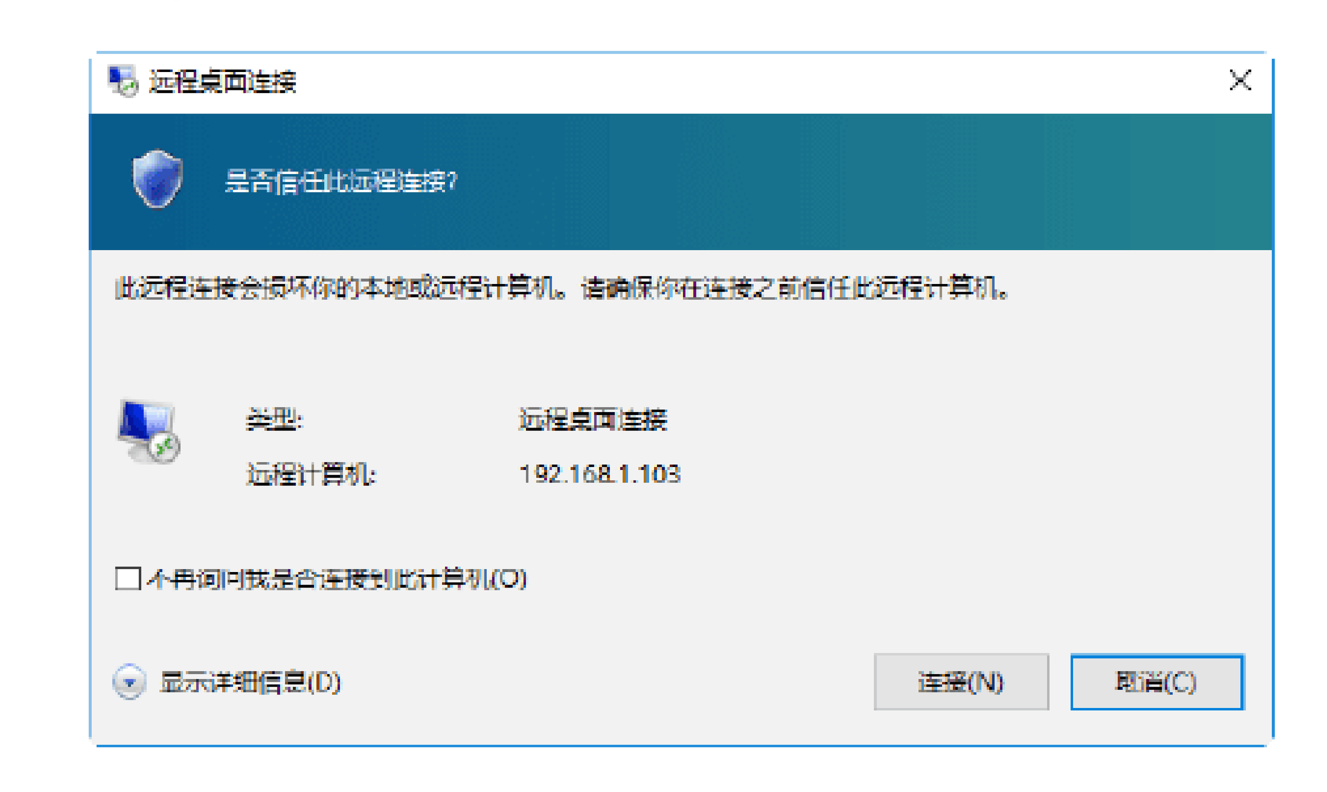
Step 04 如果需要远程桌面与本地计算机文件进行传输，则需在“本地资源”选项卡中设置相应的属性，如下图所示。



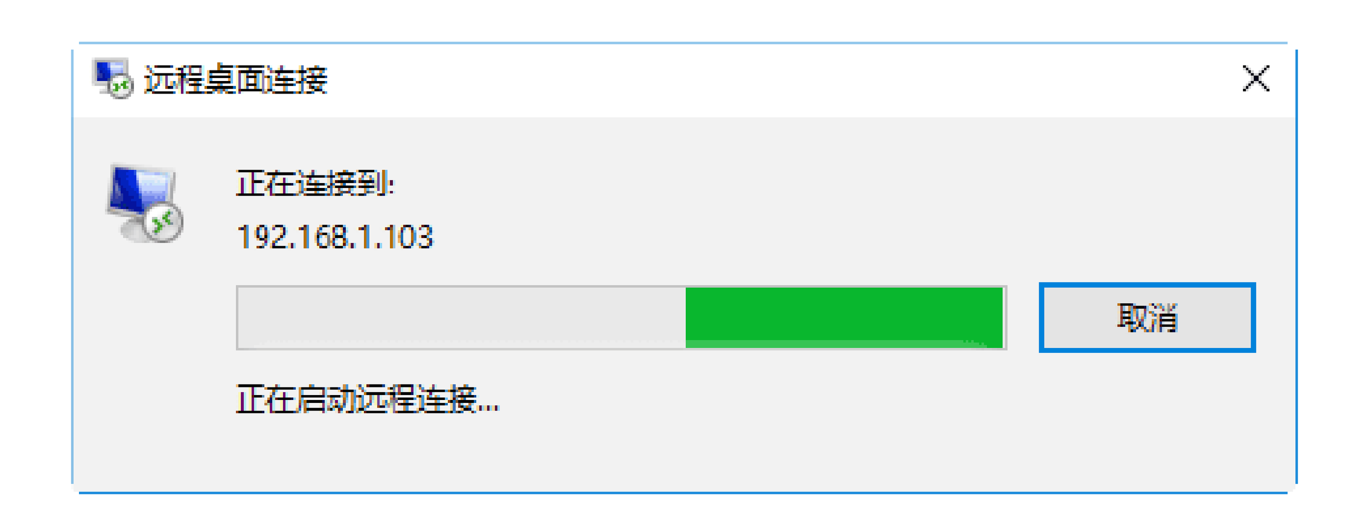
Step 05 单击“详细信息”按钮，在“本地设备和资源”中选择需要的驱动器，如下图所示，单击“确定”按钮。



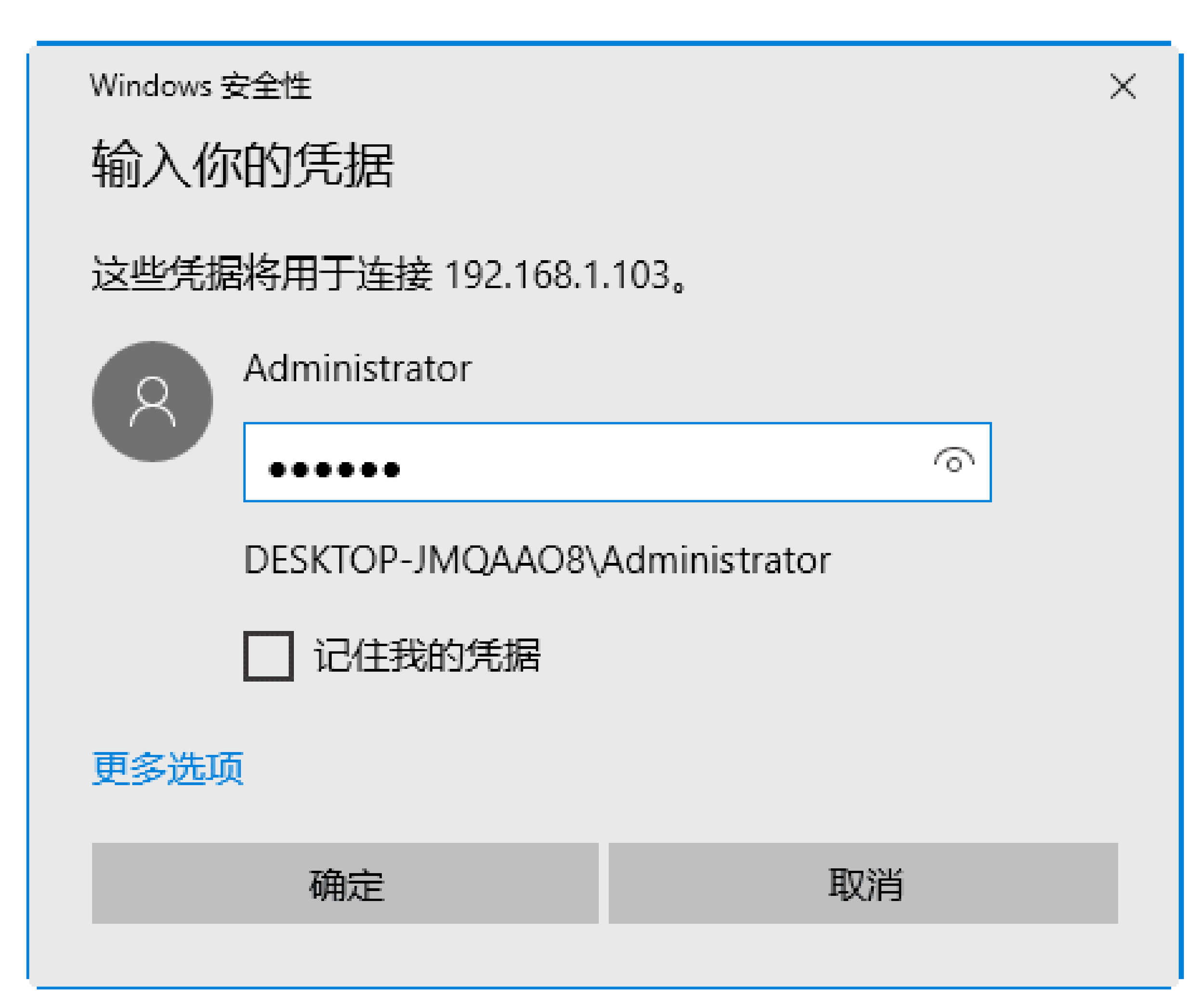
Step 06 返回到“远程桌面连接”设置窗口，单击“连接”按钮，进行远程桌面连接，如下图所示。



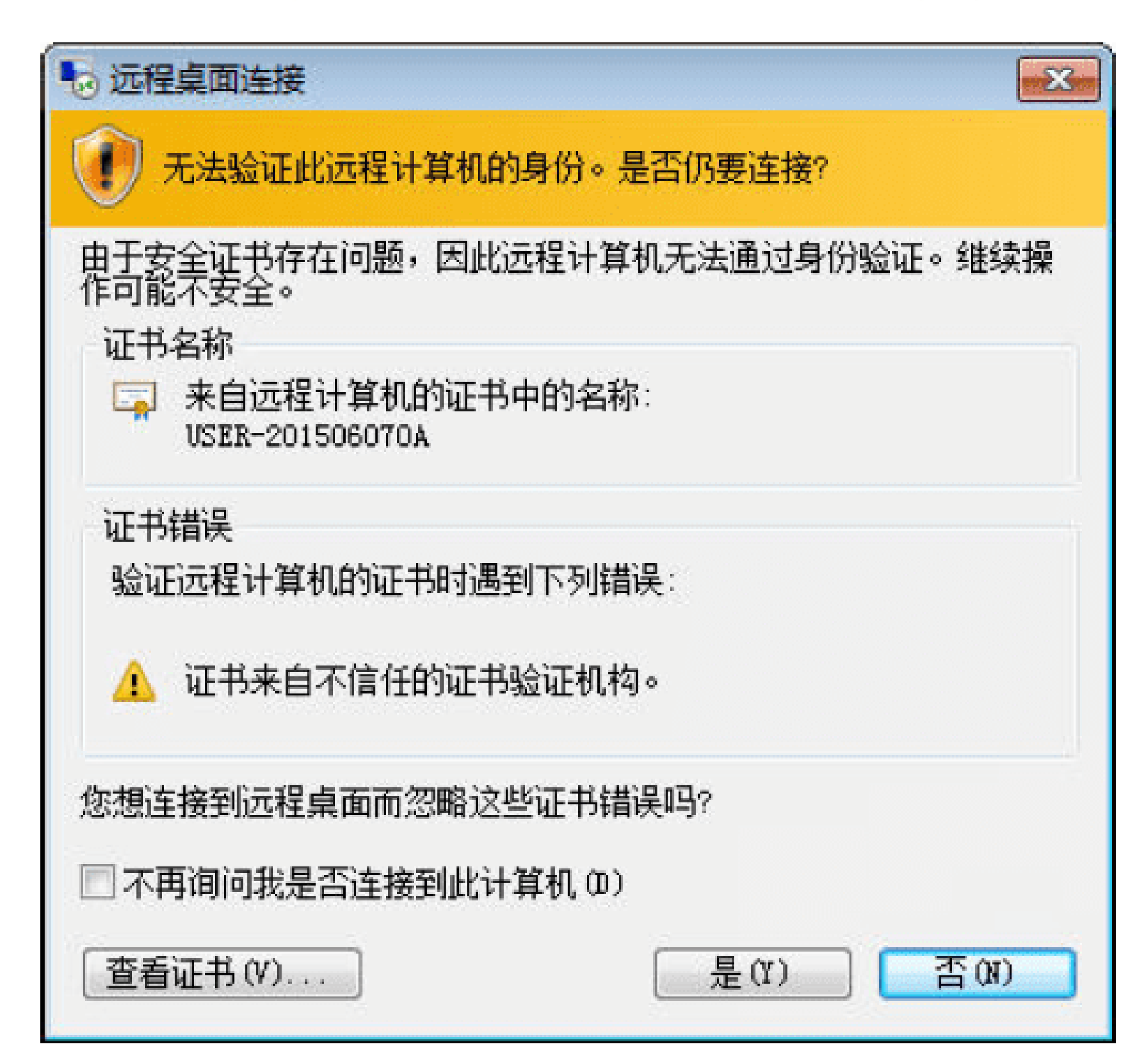
Step 07 弹出“远程桌面连接”对话框，显示正在启动远程连接，如下图所示。



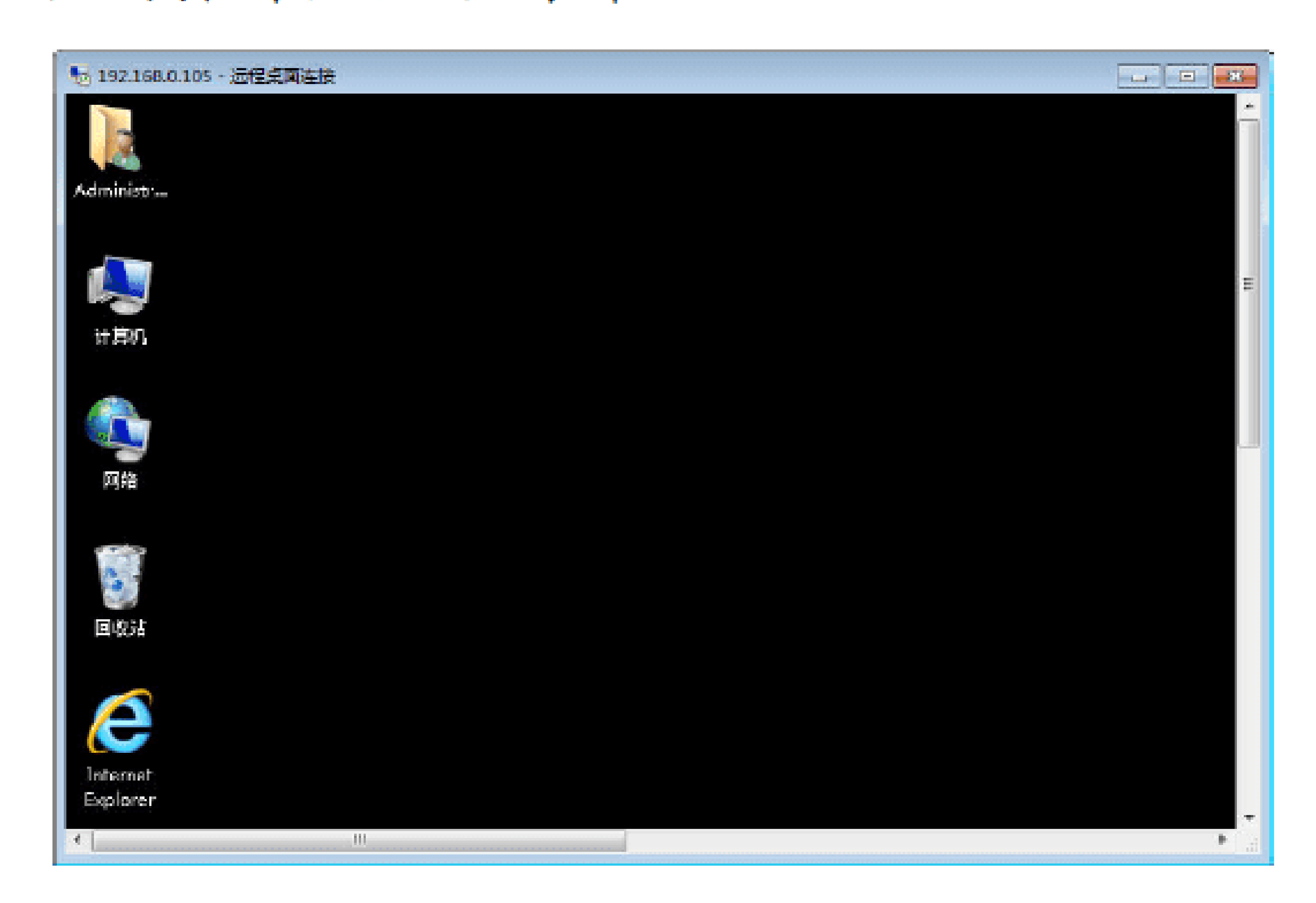
Step 08 启动远程连接完成后，将弹出“Windows安全性”对话框。在其中输入登录用户的名称与登录密码，如下图所示。



Step 09 单击“确定”按钮，弹出一个信息提示框，提示用户是否继续连接，如下图所示。



Step 10 单击“是”按钮，即可登录到远程计算机桌面，此时可以在该远程桌面上进行任何操作，如下图所示。



另外，在需要断开远程桌面连接时，只需在本地计算机中单击“远程桌面连接”窗口上的“关闭”按钮，弹出“断开与远程桌面服务会话的连接”提示框。单击“确定”按钮，即可断开远程桌面连接，如下图所示。



提示： 在进行远程桌面连接之前，需要双方都勾选“允许远程用户连接到此计算机”复选框，否则将无法成功创建连接。

6.3　使用RemotelyAnywhere入侵系统

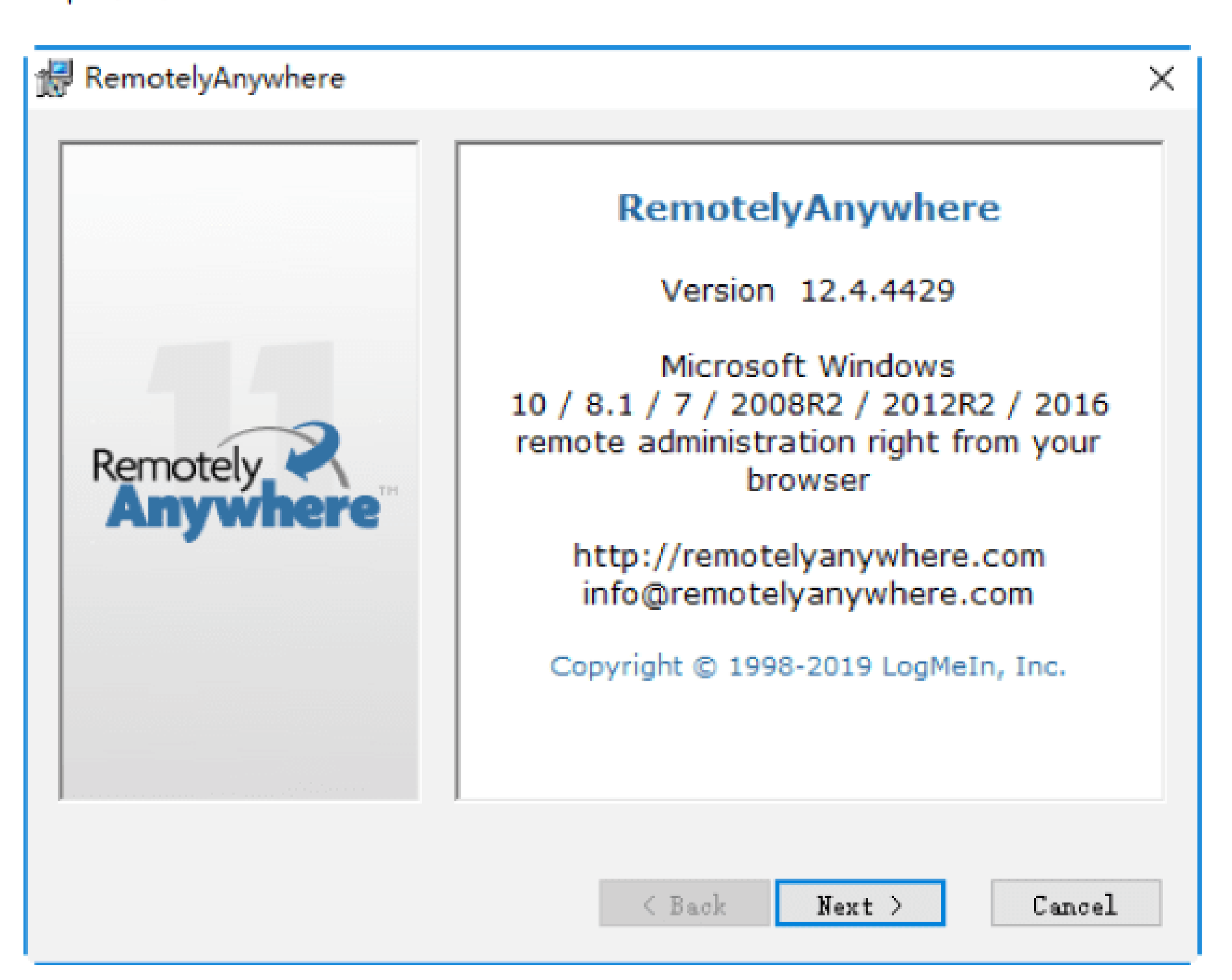
RemotelyAnywhere工具是利用浏览器进行远程连接入侵控制的小程序，使用时需要在目标主机上安装该软件，并知道该主机的连接地址以及端口，这样其他任何主机都可以通过浏览器来访问目标主机了。

实战3：安装RemotelyAnywhere

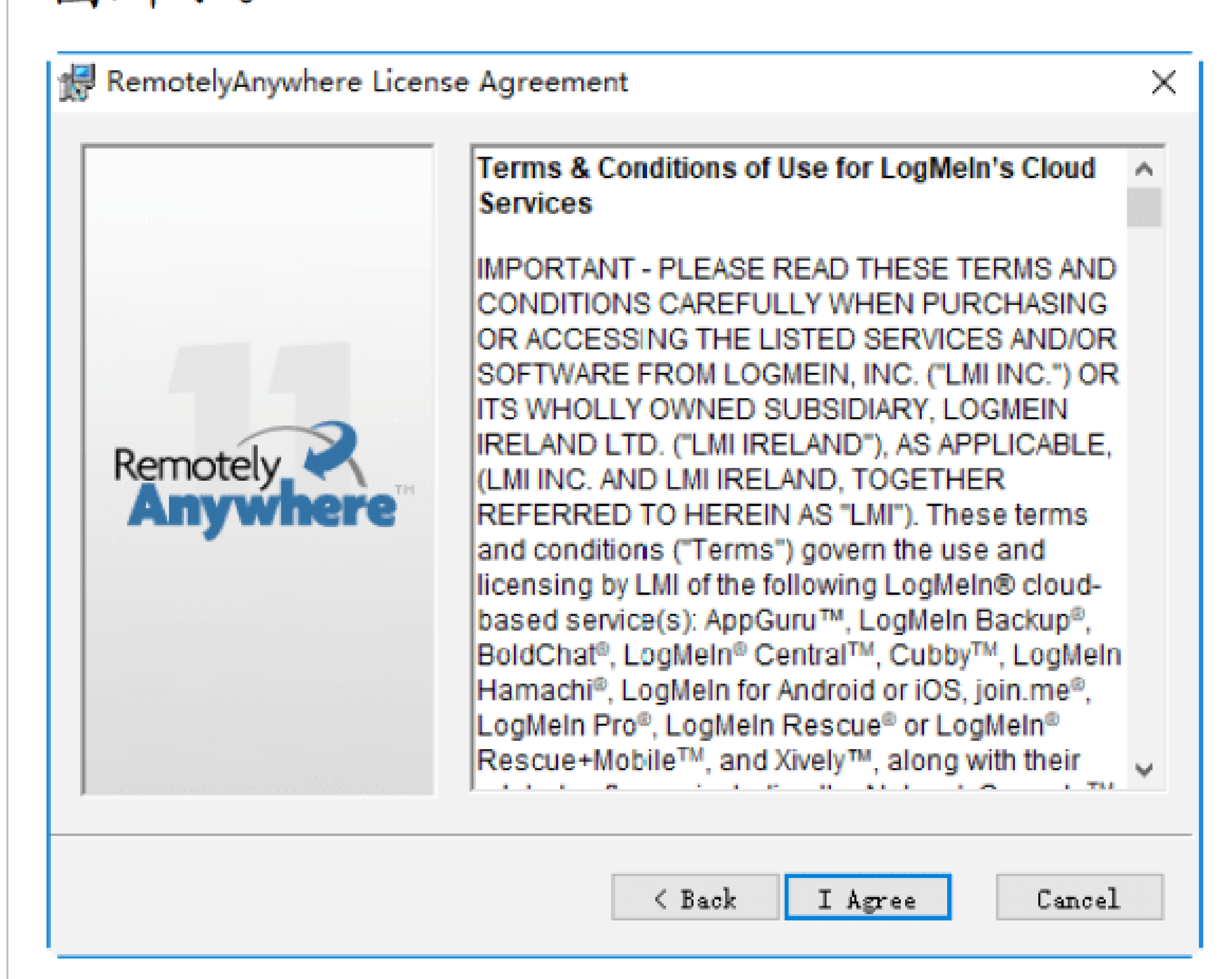


下面来学习如何安装RemotelyAnywhere软件。具体操作步骤如下。

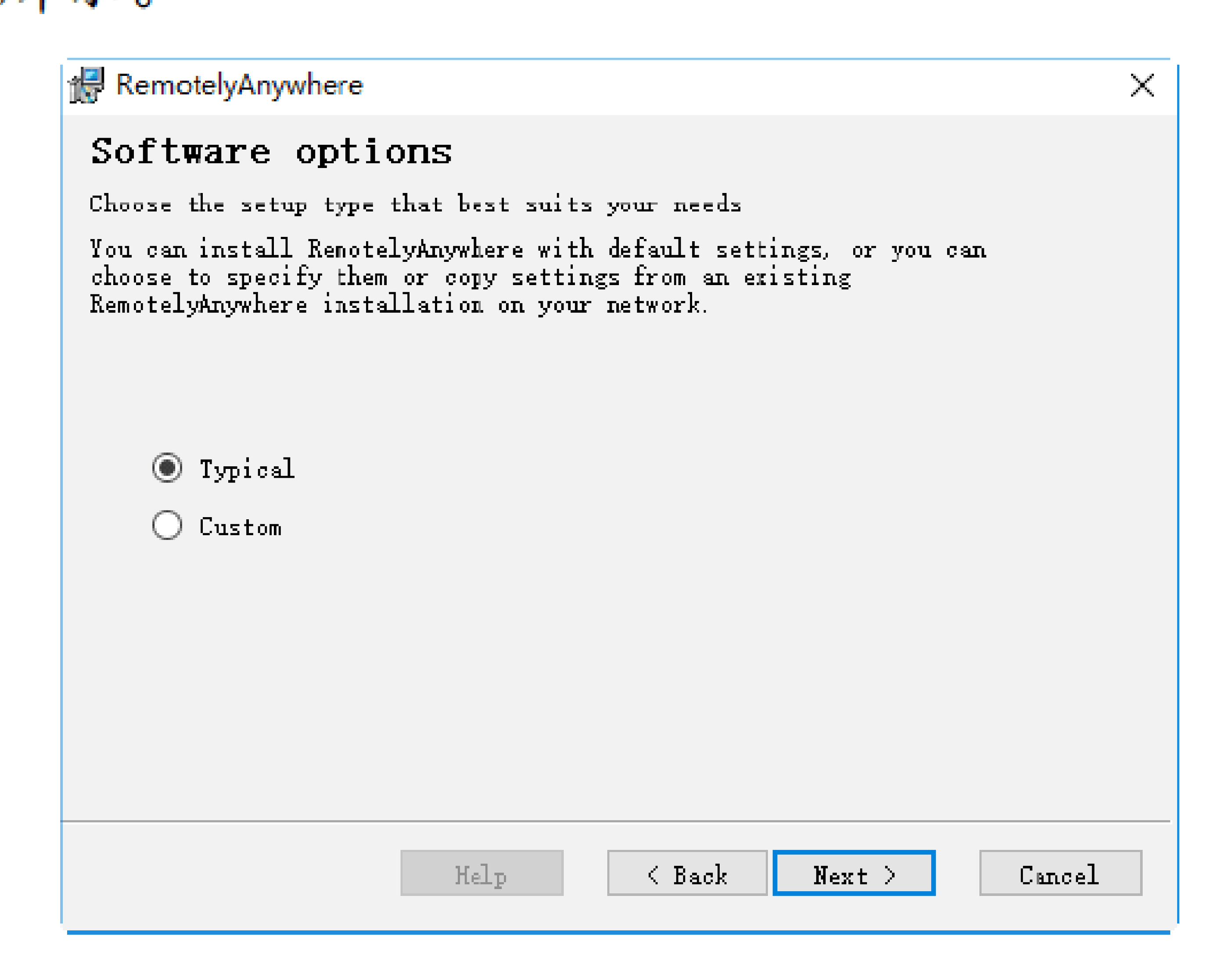
Step 01 运行RemotelyAnywhere安装程序，在弹出的对话框中单击Next按钮，如下图所示。



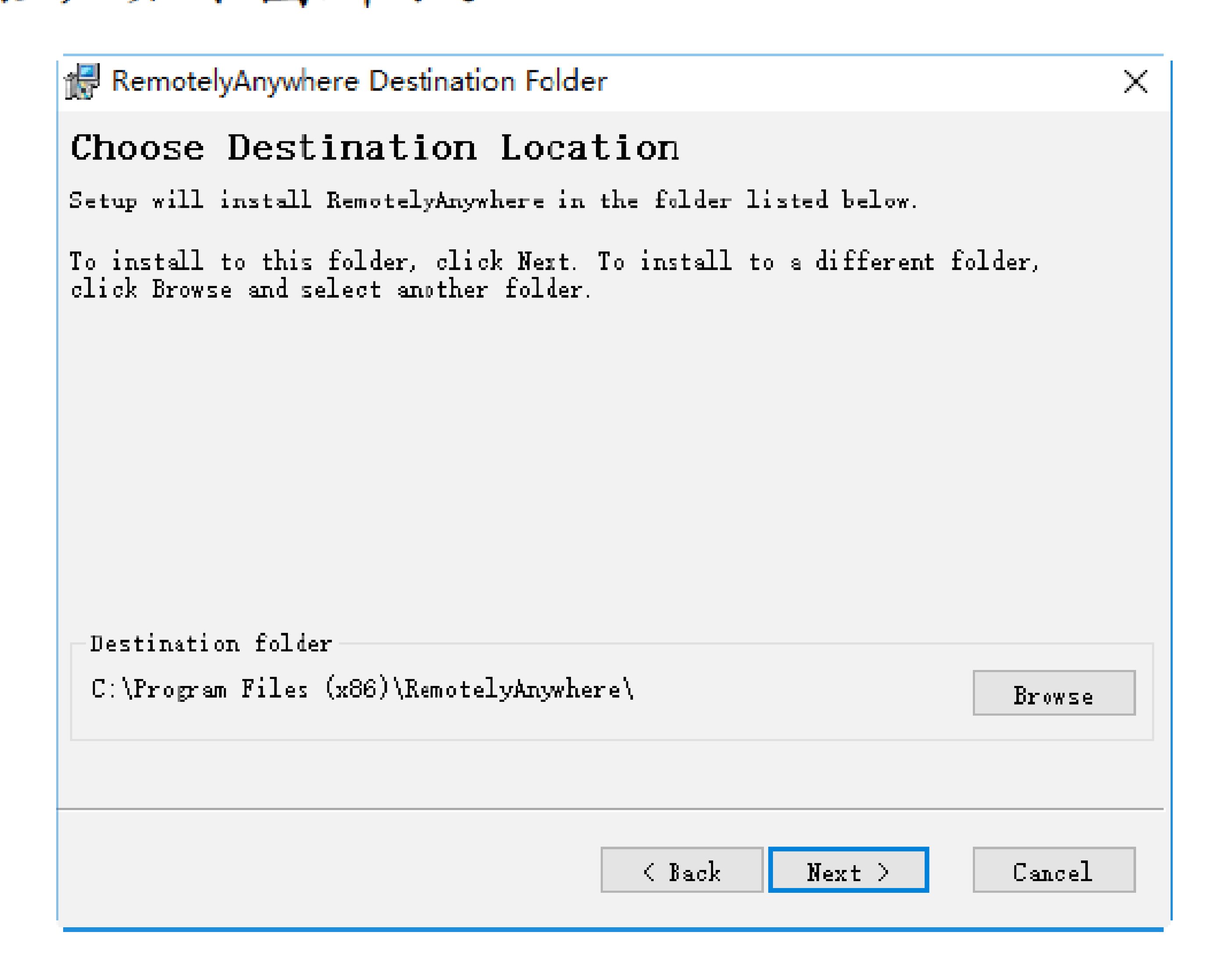
Step 02 弹出RemotelyAnywhere License Agreement对话框，单击I Agree按钮，如下图所示。



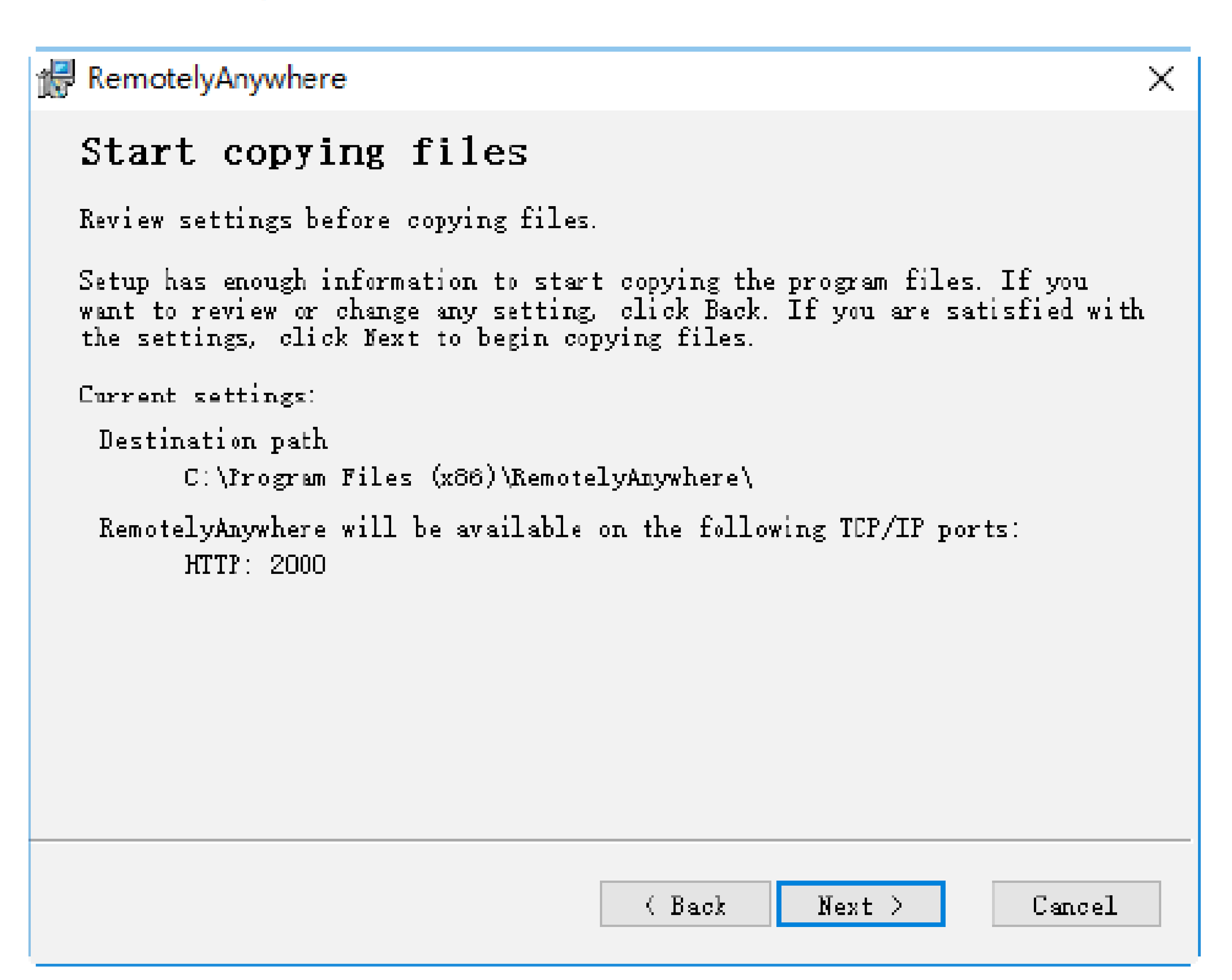
Step 03 弹出Software options对话框。选中Custom单选按钮，可以手工指定软件安装配置项，本实例选中Typical单选按钮，使用默认配置，单击Next按钮，如下图所示。



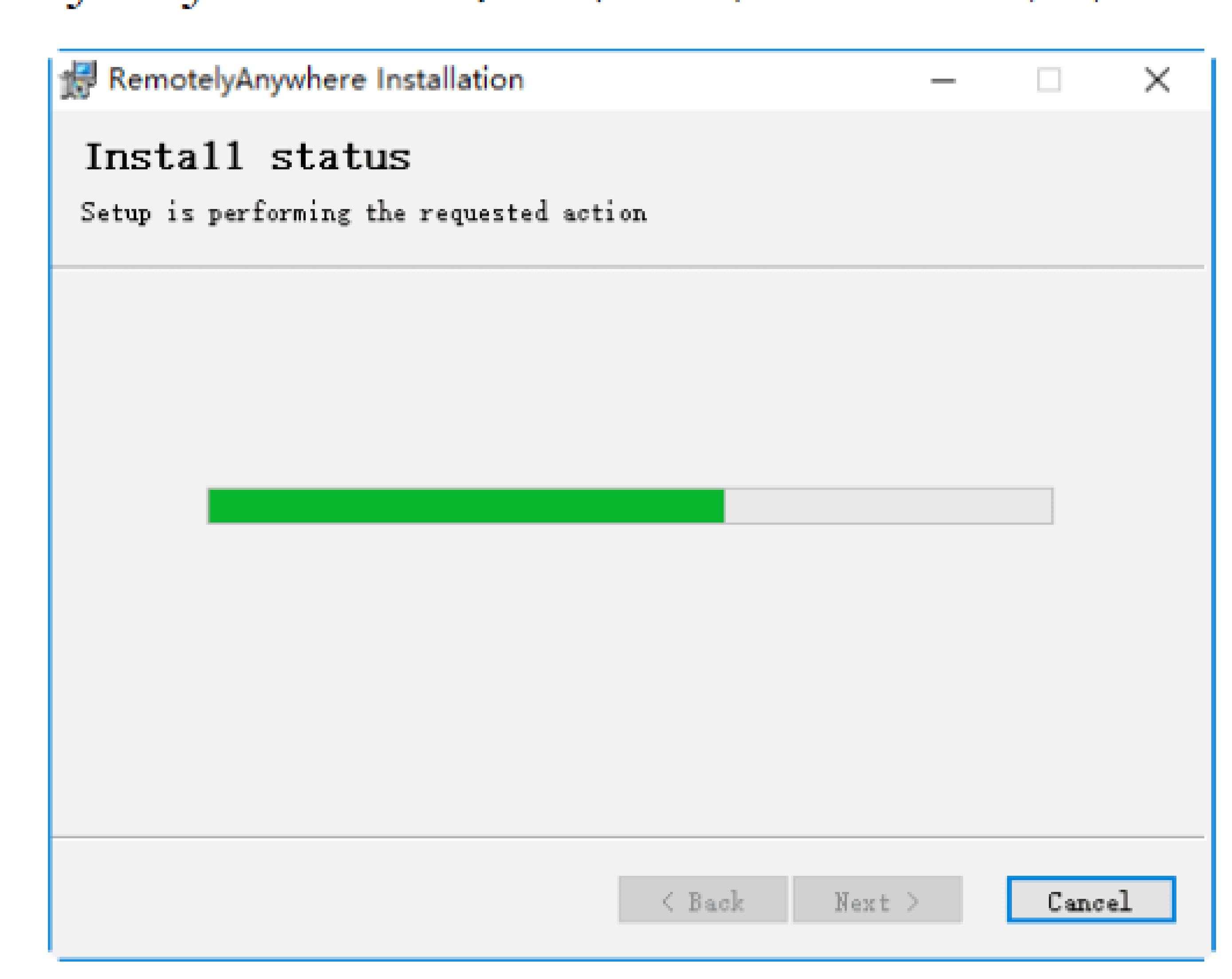
Step 04 弹出Choose Destination Location对话框，单击Browse按钮，可以改变安装目录，本实例采用默认配置，单击Next按钮，如下图所示。



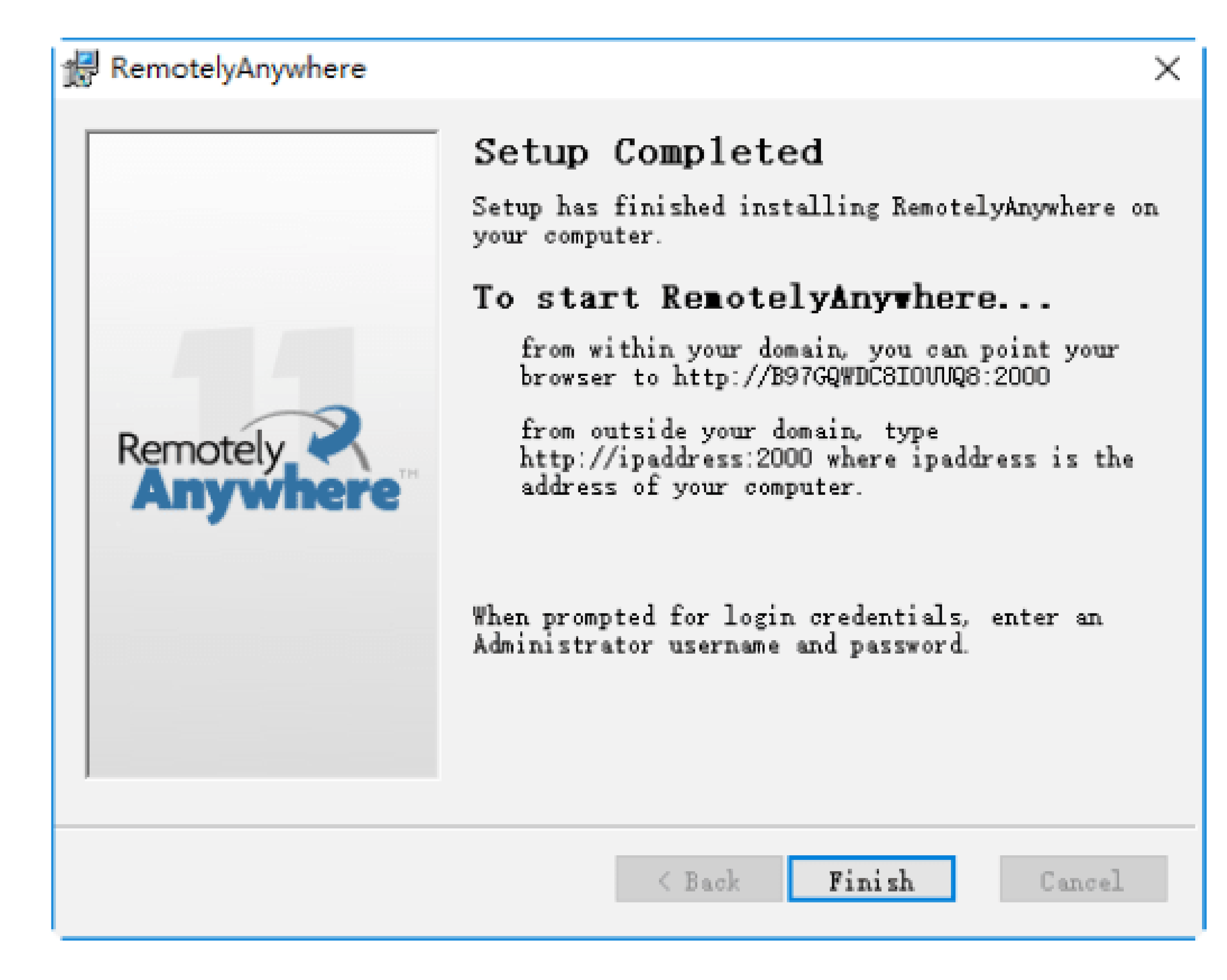
Step 05 弹出Start copying files对话框，显示已配置信息，信息中说明连接服务器的端口为2000，单击Next按钮，如下图所示。



Step 06 弹出Install status对话框，RemotelyAnywhere程序正在安装，如下图所示。



Step 07 安装完成后，弹出Setup Completed对话框，对话框中标明可以使用地址http://B97GQWDC8IOUUQ8:2000和http://ipaddress:2000连接服务器，单击Finish按钮，如下图所示。



Step 08 弹出Windows验证页面，在其中需要输入此计算机的用户名和密码，如下图所示。

Remotely Anywhere
Windows 验证
请输入此计算机的用户名和密码
用户名 Administrator
密码 •••••••••
登录
NTLM
NTLM 验证使用您当前的 Windows 登录证书来验证您针对主机的身份标识
登录
显示高级选项 >>
主机计算机的键盘和鼠标当前已激活。

Step 09 单击“登录”按钮，弹出RemotelyAnywhere激活方式选择界面，可以选中“我已是RemotelyAnywhere用户或已具有RemotelyAnywhere许可证”单选按钮进行激活，也可以选择“我希望现在购买RemotelyAnywhere”在线激活，本实例选中“我想免费试用”单选按钮，单击“下一步”按钮，如下图所示。





Step 10 在弹出界面的“电子邮件地址”文本框中输入激活使用的邮箱地址，并在“产品类型”列表选项中选择试用产品类型，本实例采用“服务器版”，单击“下一步”按钮，如下图所示。





Step 11 在弹出的界面中依次输入指定内容，单击“下一步”按钮，如下图所示。





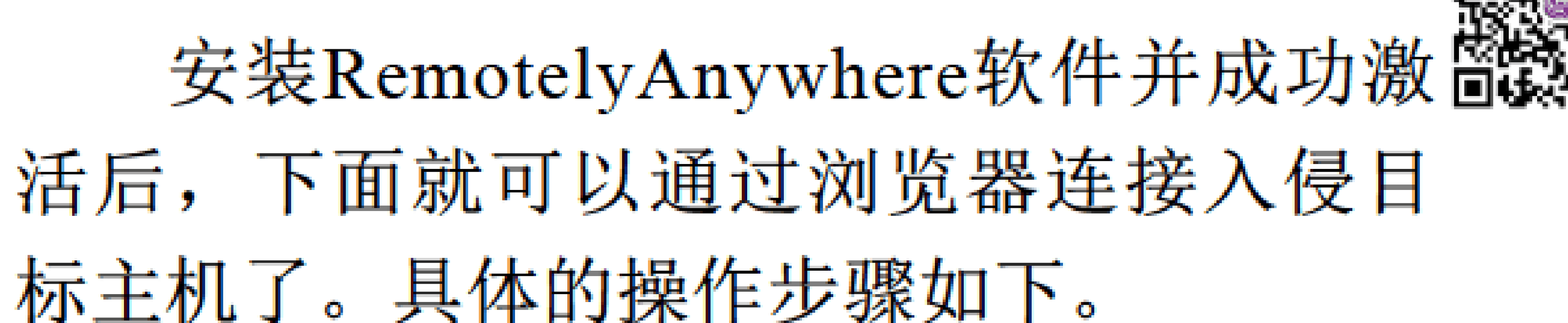
Step 12 RemotelyAnywhere激活成功，需要重新启动RemotelyAnywhere程序，单击“重新启动REMOTELYANYWHERE”按钮，如下图所示。





实战4：连接入侵远程主机





安装RemotelyAnywhere软件并成功激活后，下面就可以通过浏览器连接入侵目标主机了。具体的操作步骤如下。

Step 01 打开浏览器，在地址栏中输入RemotelyAnywhere安装过程中提示的地址，通用格式为“http://{目标服务器IP|主机名|域名}:2000”，本实例使用http://desktop-rjknmoc:2000/main.html进行讲解，在“用户名”和“密码”文本框中输入有效的远程管理账户的信息，默认使用Administrator账号登录，如下图所示。

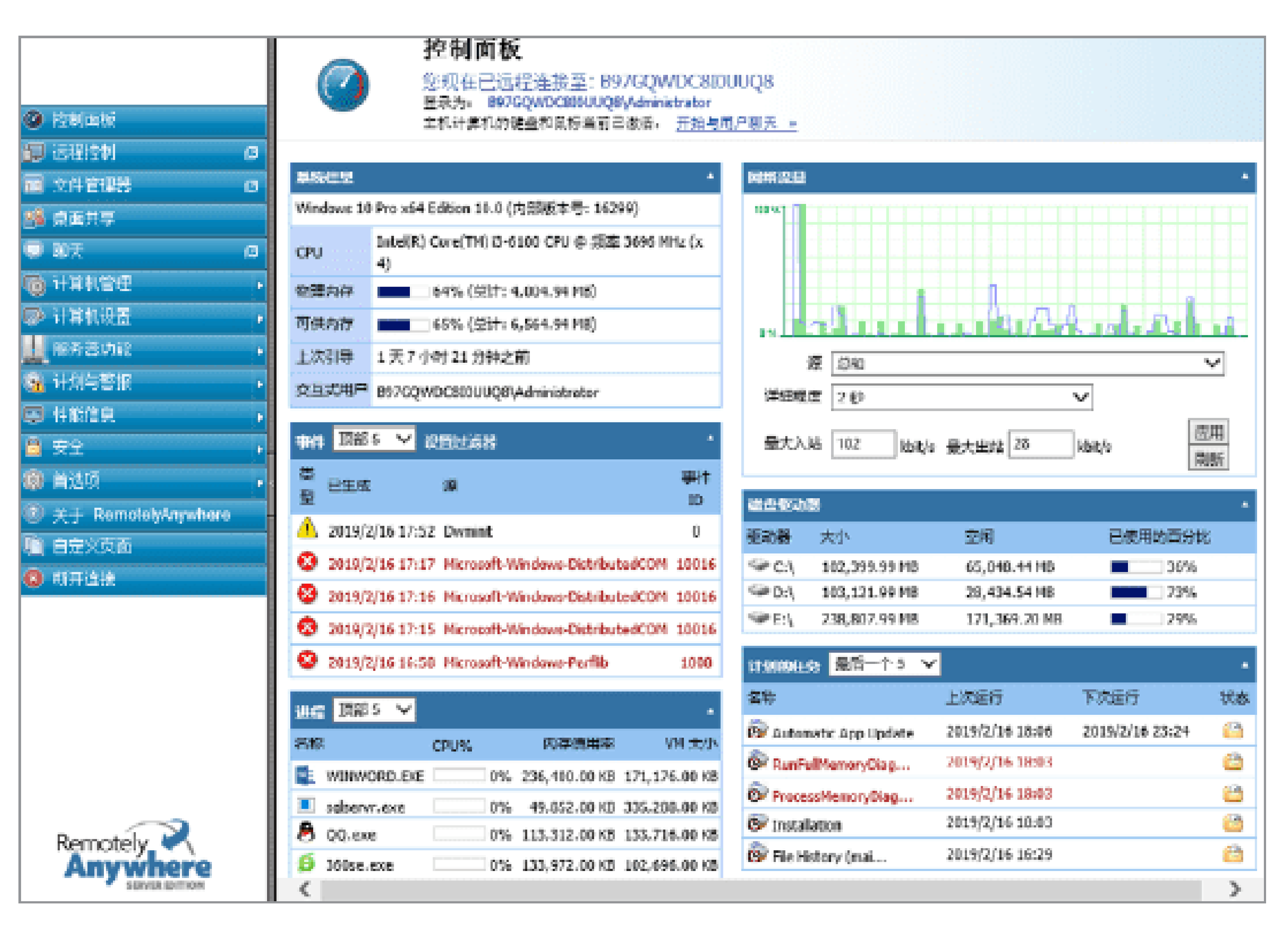
Step 02 单击“登录”按钮，进入RemotelyAnywhere远程管理界面，左侧显示管理功能列表，用户可以使用不同的管理功能对

远程主机进行多功能全方位的管理操作，如下图所示。





Step 03 单击“继续”按钮，进行远程主机信息查看与管理，默认显示“控制面板”管理功能界面，如下图所示。



通过该页面可以快速了解远程服务器的多种状态、信息，具体内容如下。

（1）系统信息：显示系统版本、CPU型号、物理内存使用情况、总内存（包括虚拟内存）使用情况、系统已启动时间、登录系统账户。

（2）事件：显示最近发生的系统事件，默认显示5个事件。

（3）进程：显示进程的系统资源占用情况，默认以CPU占用比例为序，显示CPU占用率最高的5个进程。

（4）已安装的修补程序：最近安装的系统补丁，默认显示5个补丁信息。

（5）网络流量：动态显示网络流量信息。

（6）磁盘驱动器：所有分区的空间使用情况。

（7）计划的任务：显示最后执行的任务计划，默认为5个。

（8）最近的访问：系统最近访问记录。

（9）日记：管理员可在此区域编辑管理日记。

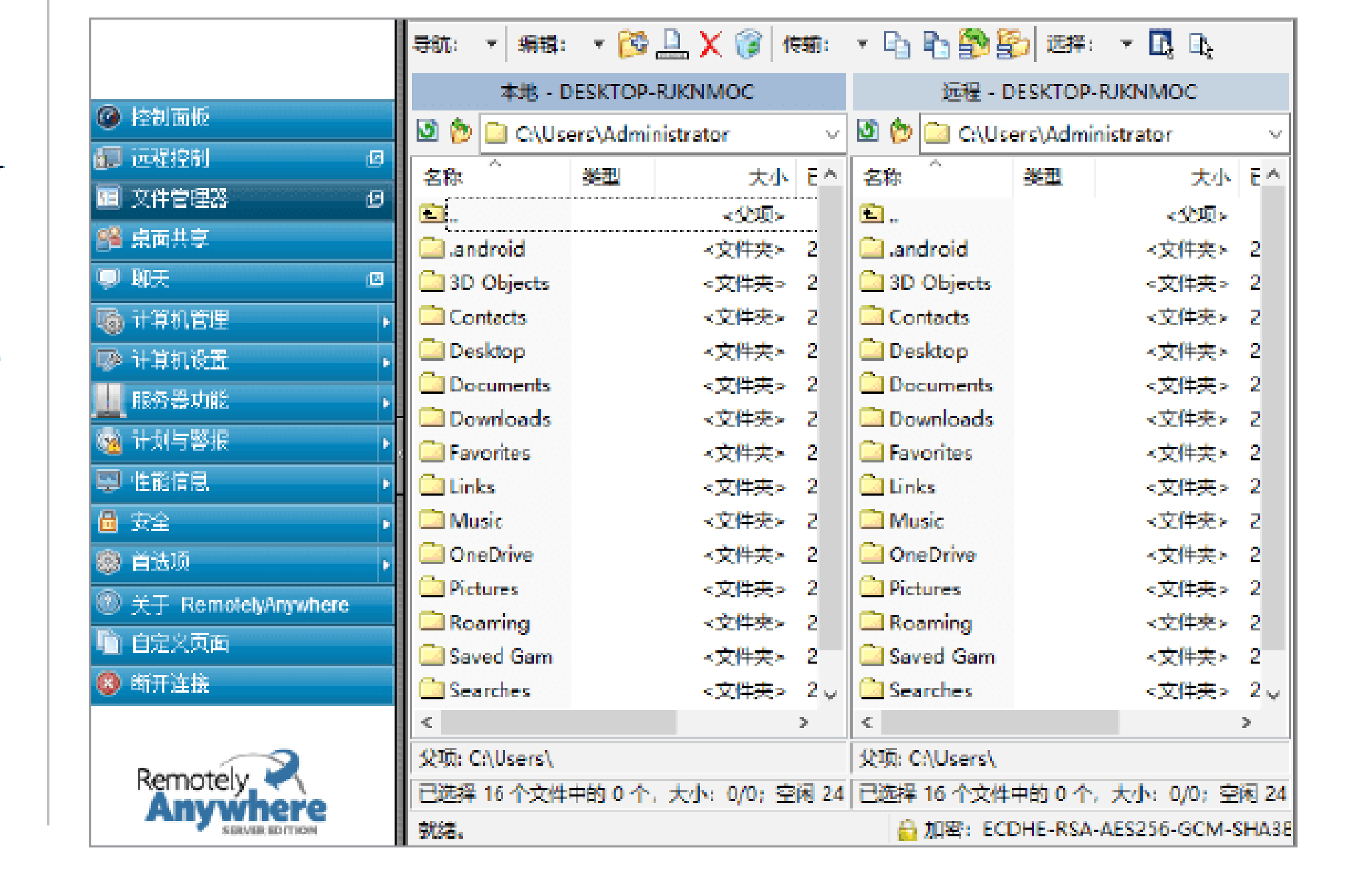
实战5：远程操控目标主机

当成功入侵目标主机后，就可以通过浏览器远程操作目标主机了。具体的操作步骤如下。

Step 01 选择左侧列表中的“远程控制”选项，在右侧窗格中显示远程主机的界面，通过该窗格可以利用本地的鼠标、键盘、显示器直接控制远程主机。在窗格上侧有部分工具可以使用，包括颜色调整、远程桌面大小调整等，如下图所示。



Step 02 选择左侧列表中的“文件管理器”选项，在右侧窗格中显示本地和远程主机的资源管理器，在两个资源管理器中可以随意地拖曳文件，以实现资料互传，如下图所示。



Step 03 选择左侧列表中的“桌面共享”选项，在右侧窗格中显示实现桌面共享的操作方法。按照提示方法右击桌面状态栏的程序图标，在弹出的快捷菜单中选择Share my Desktop选项，如下图所示。



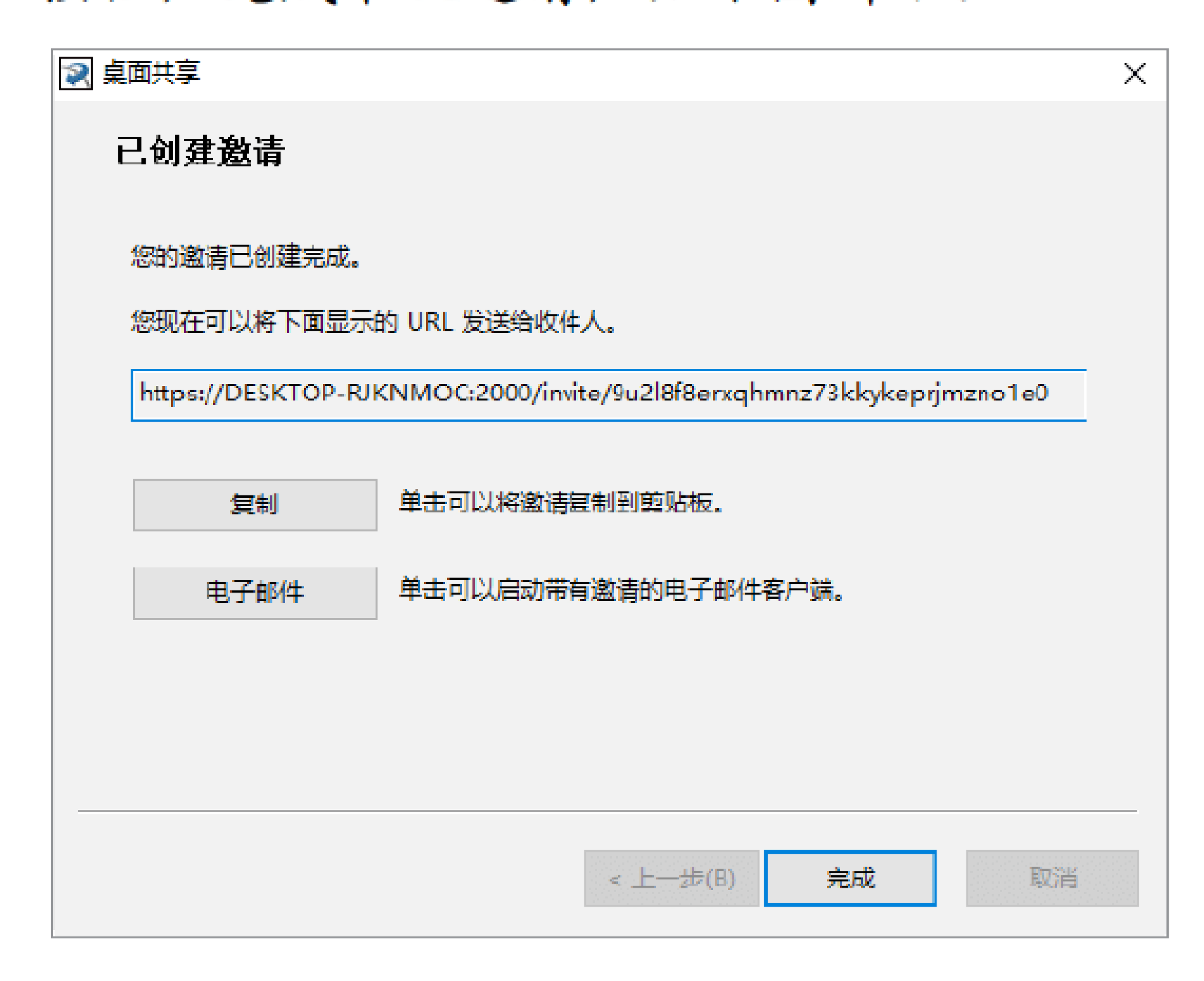
Step 04 弹出“桌面共享”对话框，选中“邀请来宾与您一起工作”单选按钮，单击“下一步”按钮，如下图所示。



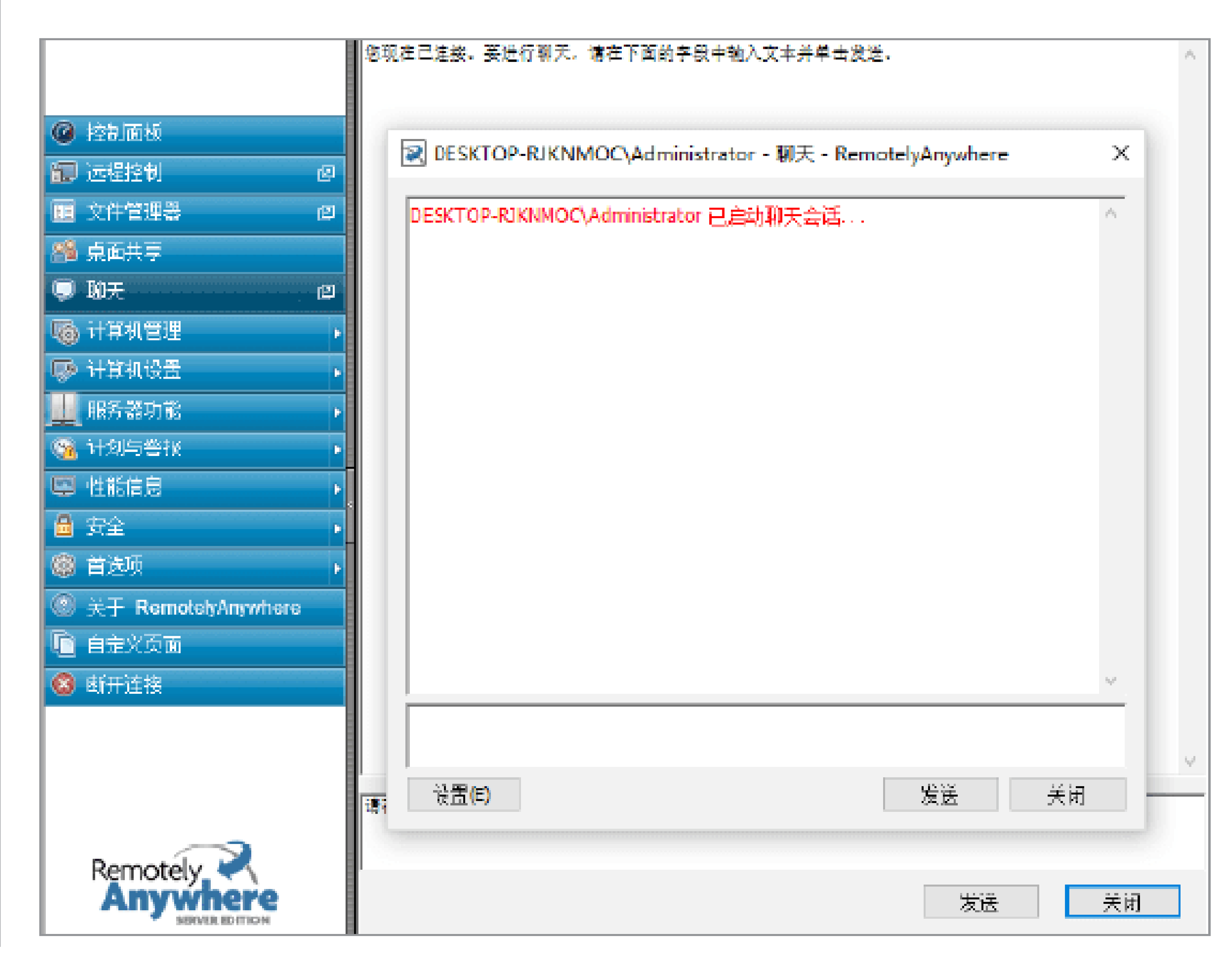
Step 05 弹出“邀请详情”对话框，可以在本对话框中配置邀请名，默认按时间显示，方便以后查看，还可以设置本次邀请的有效访问时限，在最后一个文本框中输入被邀请人连接目标主机使用的地址，全部选择默认配置，单击“下一步”按钮，如下图所示。



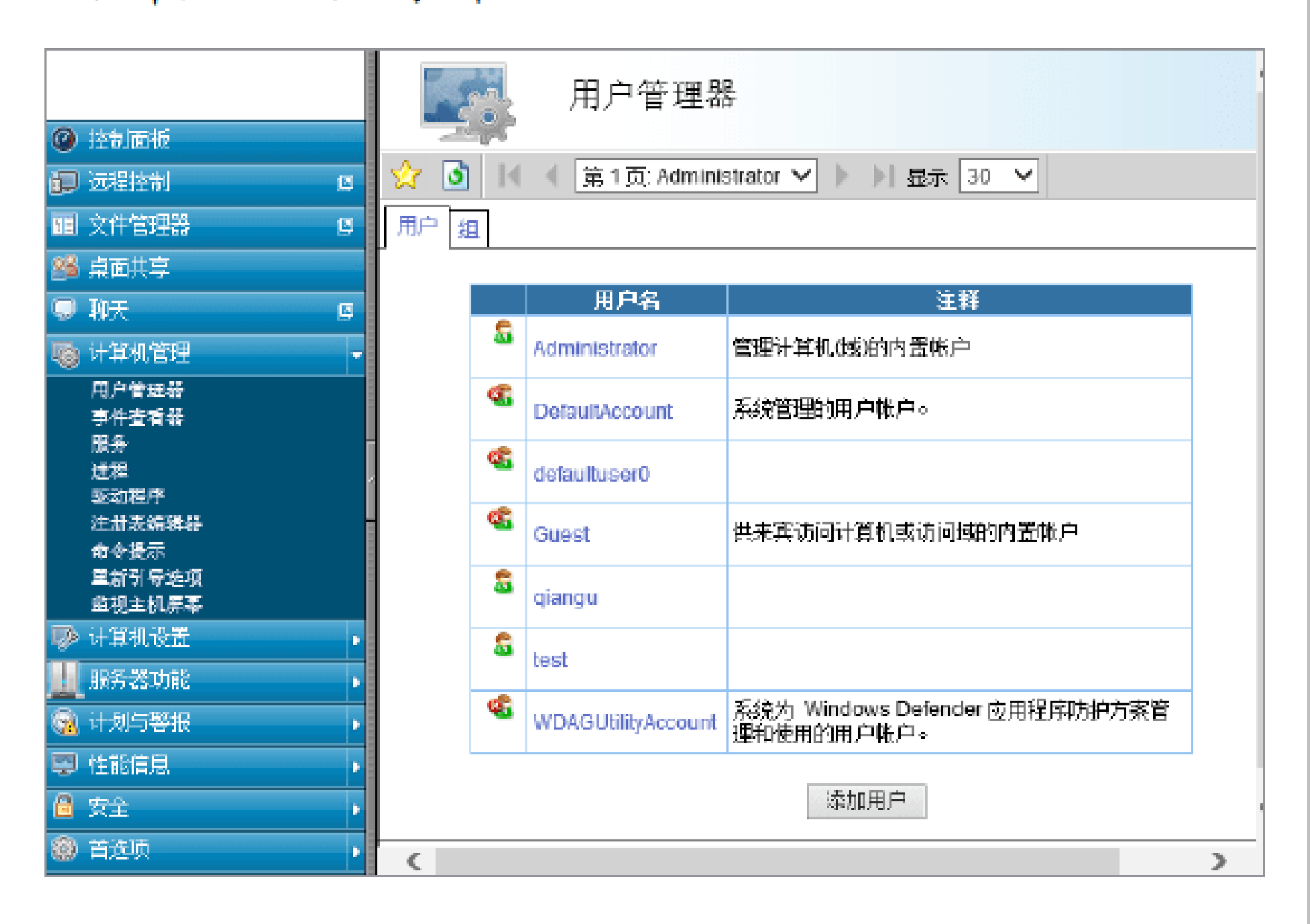
Step 06 弹出“已创建邀请”对话框，在文本框中显示被邀请人获得的地址，可以通过单击“复制”和“电子邮件”两个按钮，让被邀请人获得邀请地址，单击“完成”按钮，完成本次邀请，如下图所示。



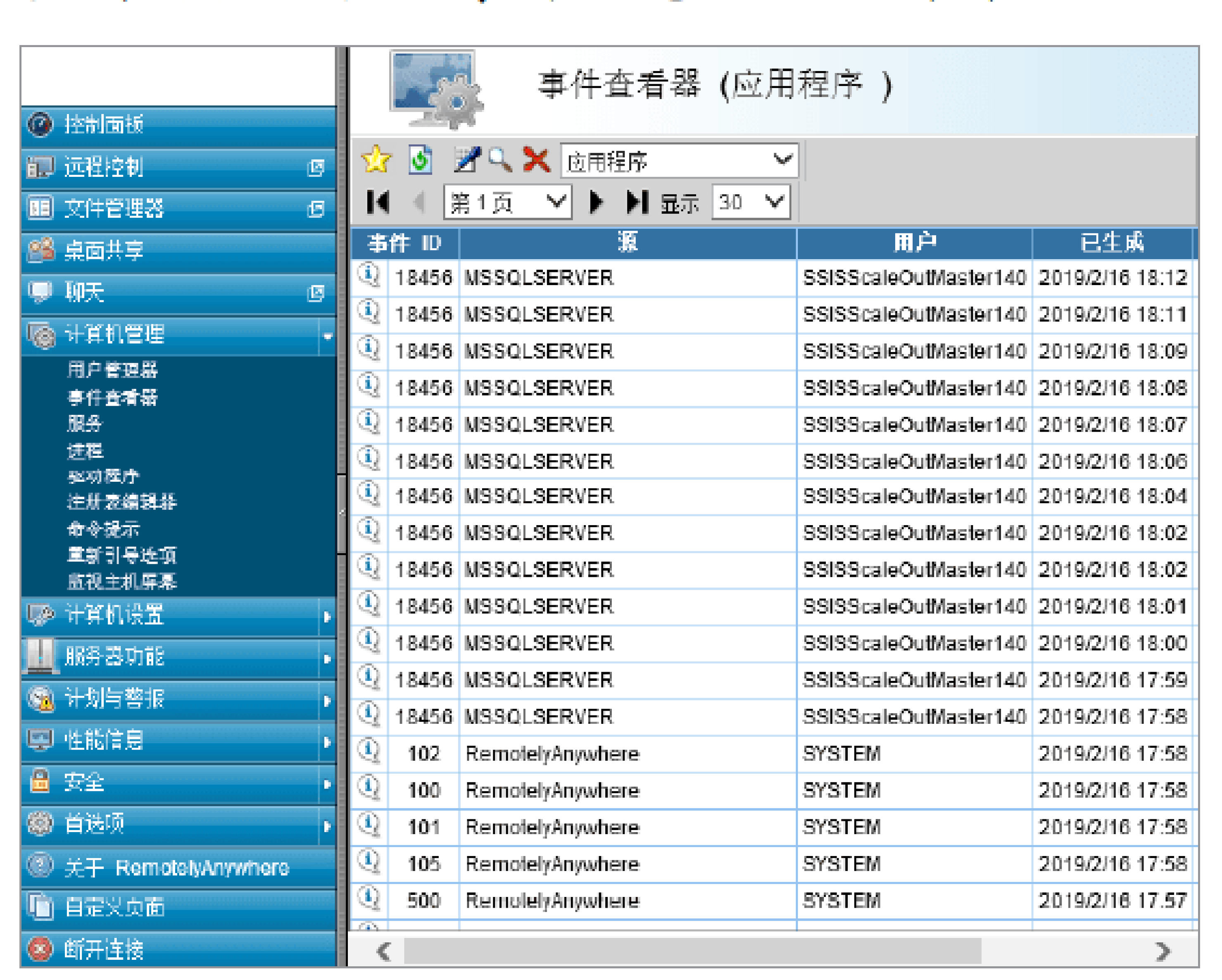
Step 07 单击左侧列表中“聊天”选项，如下图所示，通过右侧窗格可以与被管设备聊天，一般被管设备很少有人在，所以该功能用得比较少。



Step 08 选择左侧列表中的“计算机管理”→“用户管理器”选项，在右侧“用户管理器”窗格中显示远程主机的用户和组信息，单击“添加用户”按钮可以为远程主机增加用户，同时可以对用户名进行编辑，如下图所示。

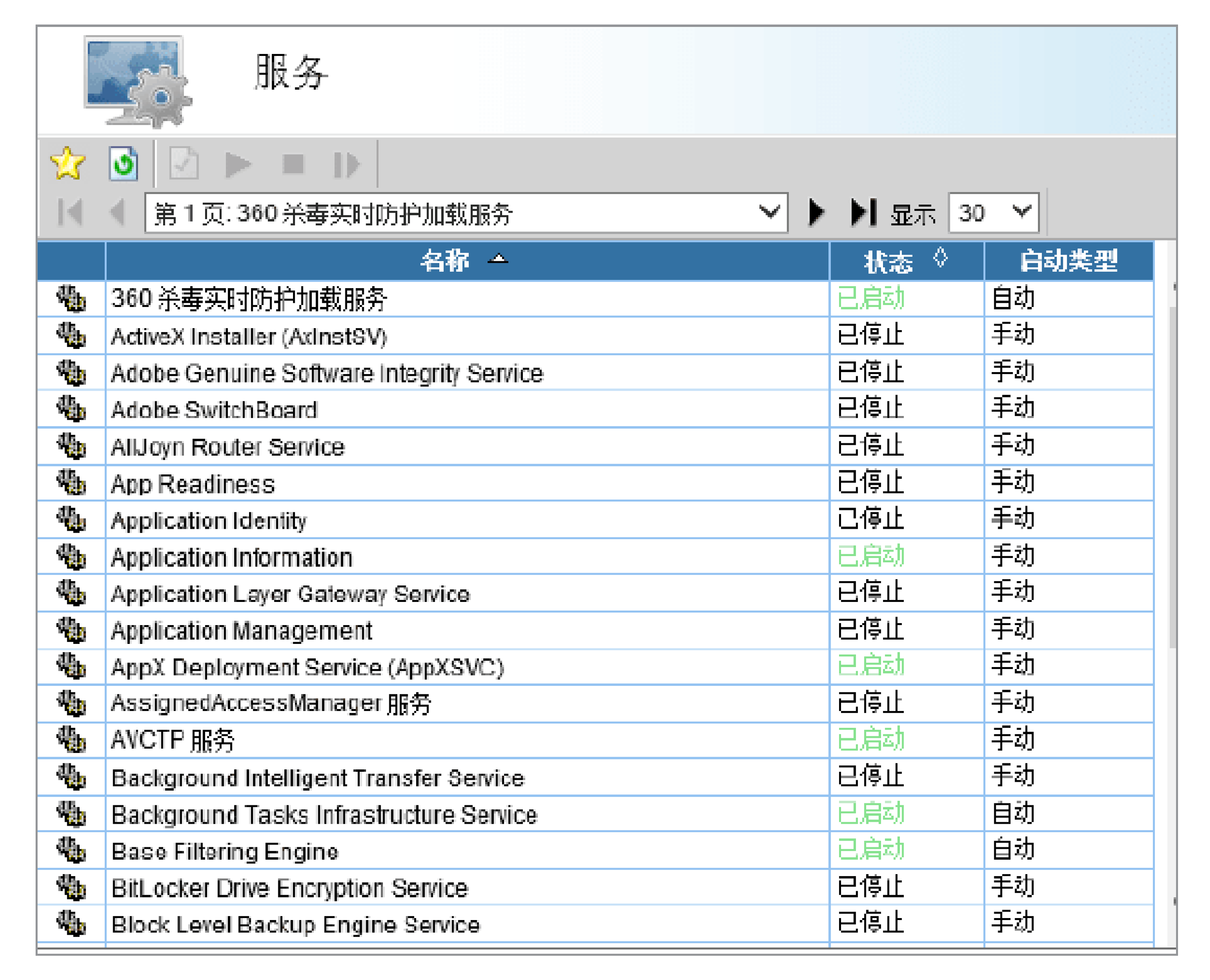


Step 09 选择左侧列表中的“计算机管理”→“事件查看器”选项，在右侧窗格中显示“事件查看器”窗格，通过该窗格可以查看远程主机的事件信息，如下图所示。



Step 10 选择左侧列表中的“计算机管理”→“服务”选项，在右侧窗格中显示“服务”窗格，通过该窗格可以查看远程主机所有的服务项，也可以单击这些服务项进行启动、禁用和删除操作，如下图所示。

Step 11 选择左侧列表中的“计算机管理”→“进程”选项，在右侧窗格中显示“进程”窗格，通过该窗格可以查看远程主机所有的进程，如下图所示，单击PID号为1016的进程。

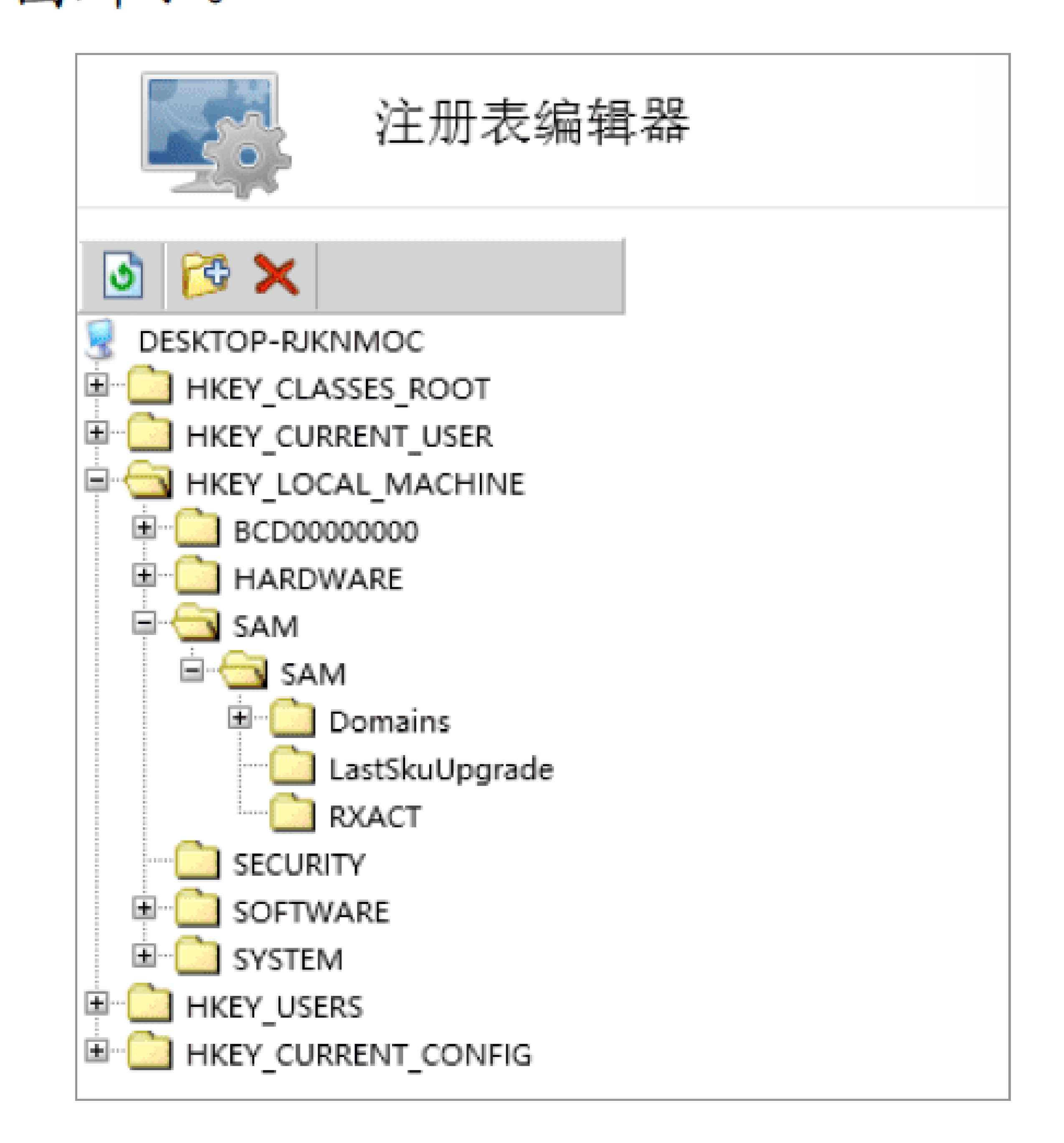




Step 12 弹出新页面，显示出进程1016的进程名为WUDFHost.exe，同时还显示了该进程的其他信息。通过修改“优先级类”下拉菜单选项，可以调整该进程的优先级别，可以为需要优先执行的进程做调整，如下图所示。



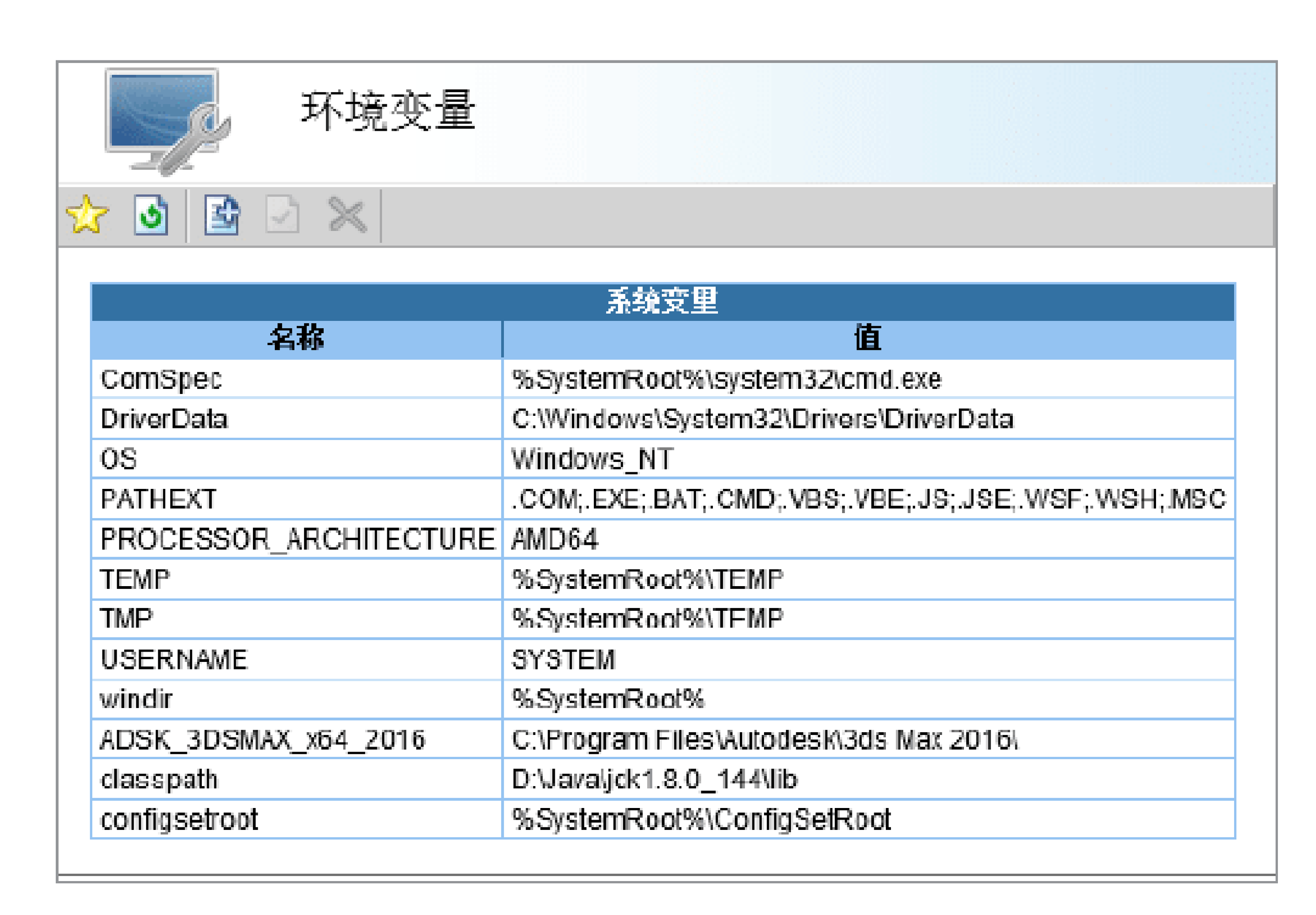
Step 13 选择左侧列表中的“计算机管理”→“注册表编辑器”选项，在右侧窗格中显示“注册表编辑器”窗格，通过该窗格可以查看远程主机的注册表信息，如下图所示。



Step 14 选择左侧列表中的“计算机管理”→“重新引导选项”，在右侧窗格中显示“重新引导选项”窗格，如下图所示，通过该窗格可以根据需求对远程主机做各种引导操作，只需要单击指定的图标按钮即可。



Step 15 选择左侧列表中的“计算机设置”→“环境变量”选项，在右侧窗格中显示“环境变量”窗格，如下图所示，通过该窗格可以修改远程主机的环境变量信息，单击指定环境变量选项进行调整即可。


环境变量

系统变量	
名称	值
ComSpec	%SystemRoot%\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
OS	Windows_NT
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64
TEMP	%SystemRoot%\TEMP
TMP	%SystemRoot%\TEMP
USERNAME	SYSTEM
windir	%SystemRoot%
ADSK_3DSMAX_x64_2016	C:\Program Files\Autodesk\3ds Max 2016\
classpath	D:\Java\jdk1.8.0_144\lib
configsetroot	%SystemRoot%\ConfigSetRoot

Step 16 选择左侧列表中的“计算机设置”→“虚拟内存”选项，在右侧窗格中显示“虚拟内存”窗格，如下图所示，通过该窗格可以修改远程主机的不同磁盘驱动器提供虚拟内存的数量。建议不要选择C盘，总量设置为物理内存的1.5倍，单击“应用”按钮使配置生效。

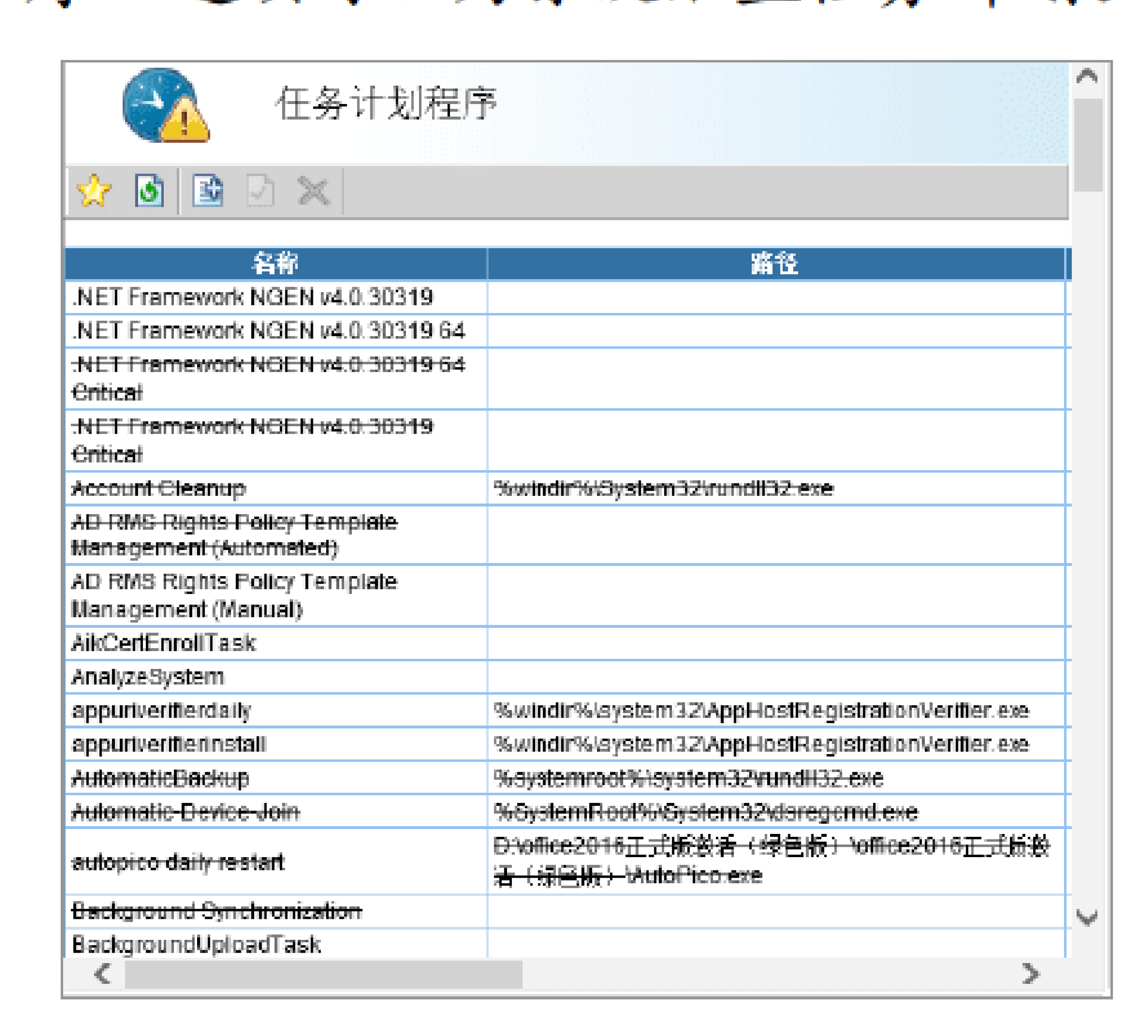


Step 17 通过RemotelyAnywhere还可以改变个别主机的配置，如FTP、活动目录，如下图所示。不过该功能一般不建议使用。

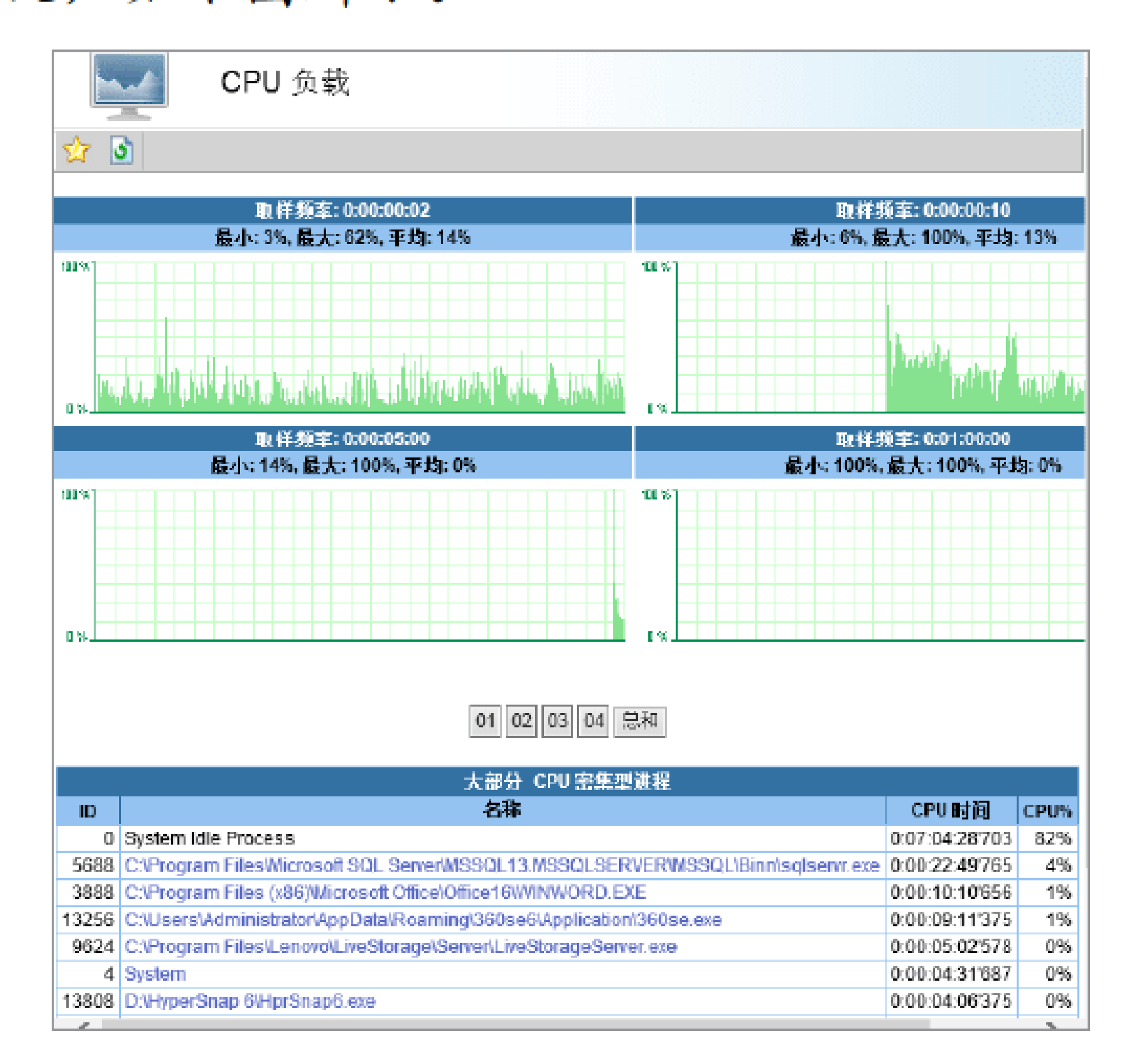


Step 18 在左侧选项列表中选择“计划与警报”选项，该选项有两个子选项，分别是“电子邮件警报”和“任务计划程序”，如下图所示。通过“电子邮件警报”选项可以监视系

统接收的电子邮件信息，对垃圾邮件等有安全威胁的信息提供警报提示；通过“任务计划程序”选项可以为系统配置任务计划。

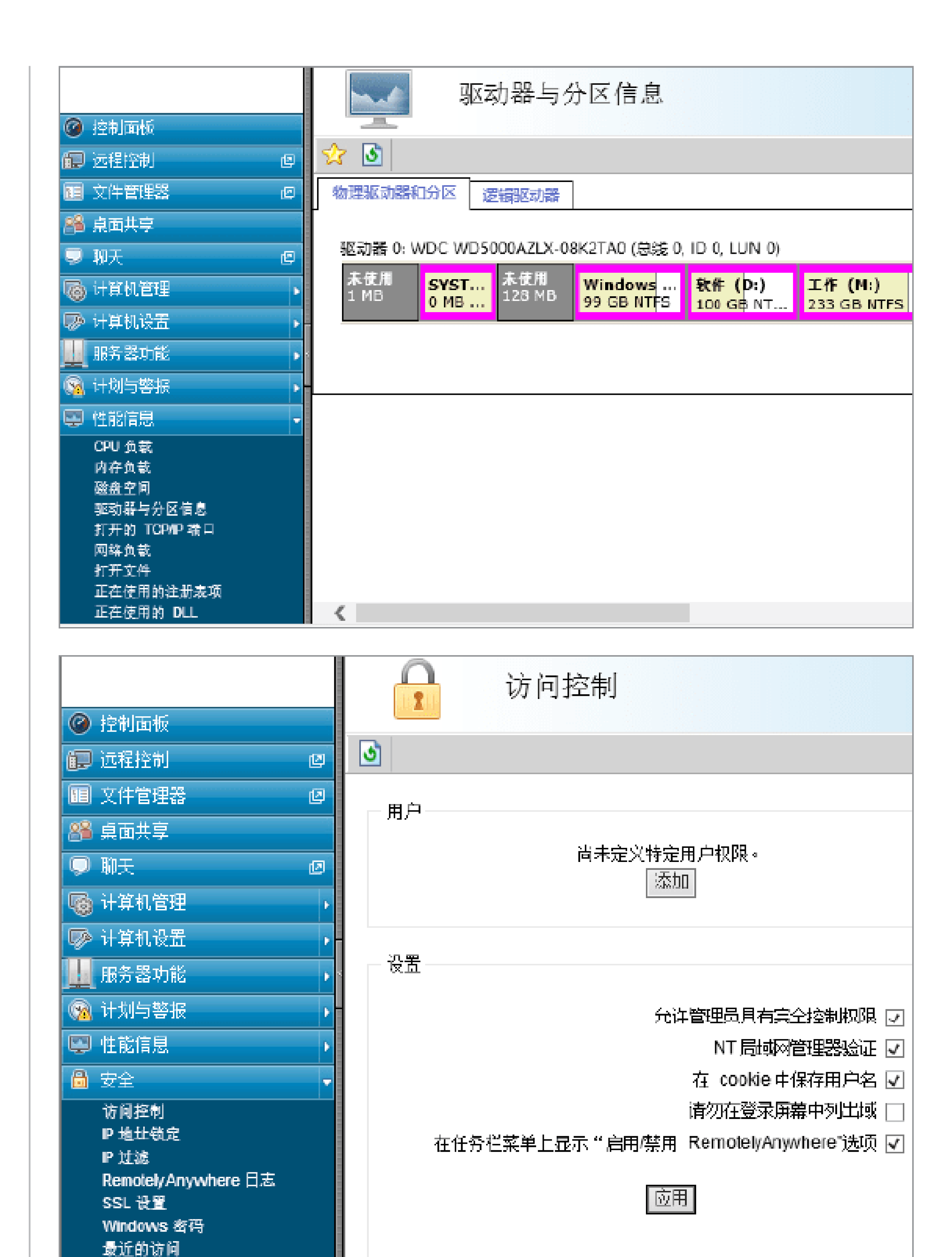


Step 19 在左侧选项列表中选择“性能信息”→“CPU负载”选项，在右侧显示“CPU负载”窗格，该窗格显示CPU的使用图表，从表中可以看到各个进程的CPU使用情况，如下图所示。

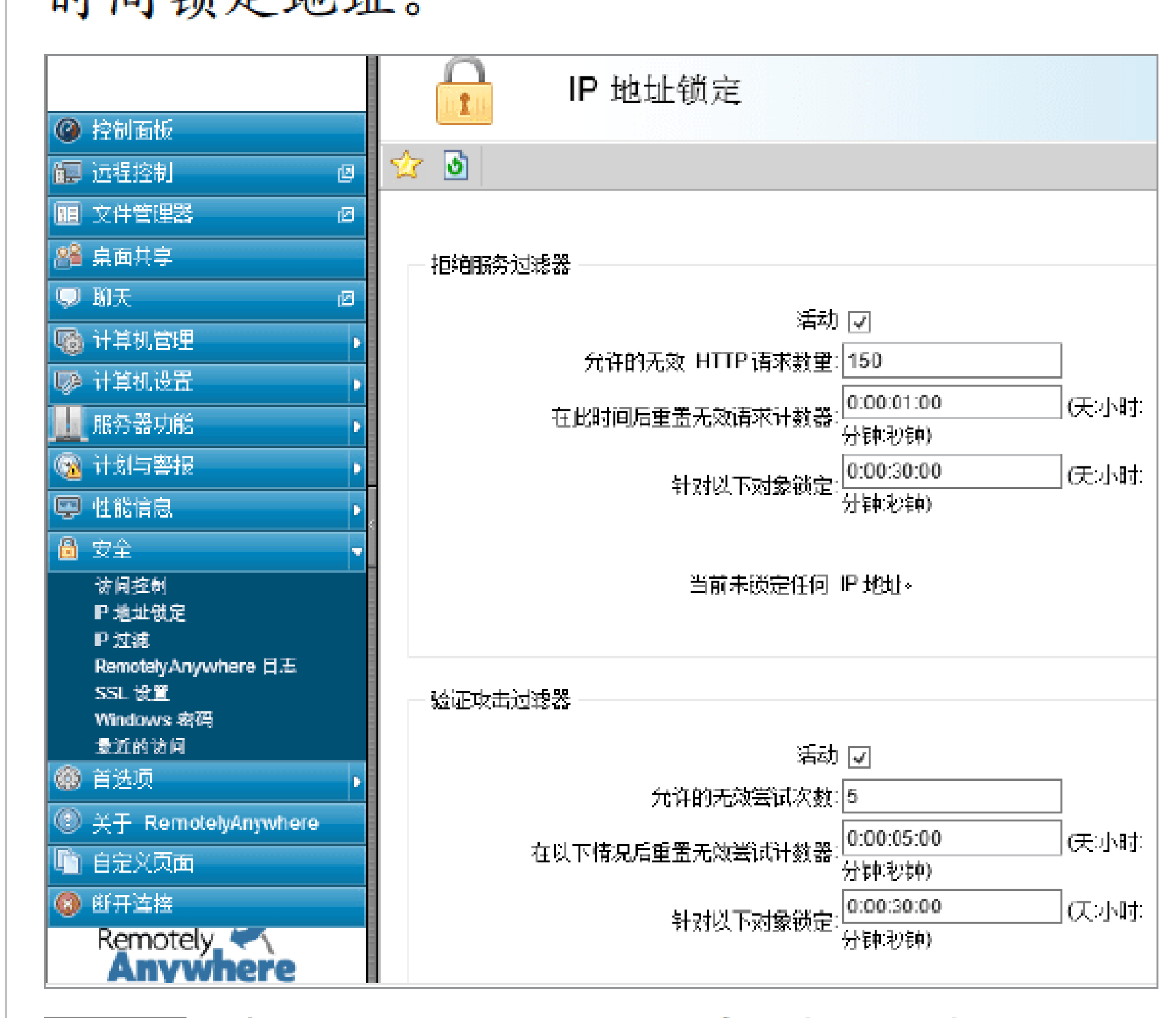


Step 20 在左侧选项列表中选择“性能信息”→“驱动器与分区信息”选项，在右侧显示“驱动器与分区信息”窗格，该窗格显示远程主机磁盘分区情况及各个分区的状态信息，可以单击指定分区进行分区调整，如下图所示。

Step 21 在左侧选项列表中选择“安全”→“访问控制”选项，在右侧显示“访问控制”窗格，如下图所示，通过该窗格可以设置部分访问控制内容，如为特定用户指定访问权限。配置完成后单击“应用”按钮生效。

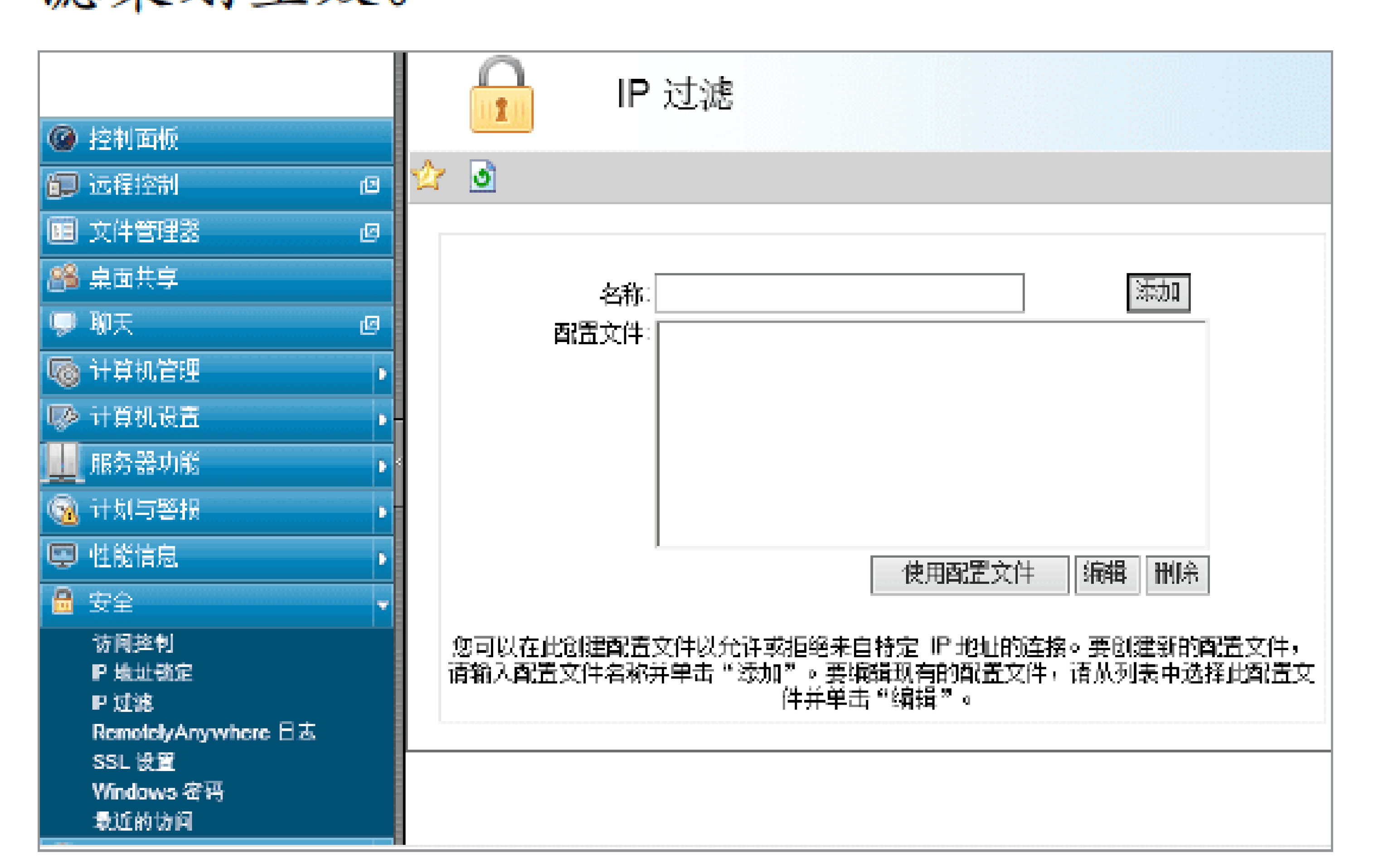


Step 22 在左侧选项列表中选择“安全”→“IP地址锁定”选项，在右侧显示“IP地址锁定”窗格，如下图所示，通过该窗格可以对非法访问远程主机的地址进行锁定操作。“拒绝服务过滤器”根据对服务器HTTP无效请求数进行IP地址锁定；“验证攻击过滤器”根据对服务器无效验证数进行IP地址锁定，超出阀值的按照规定时间锁定地址。



Step 23 在左侧选项列表中选择“安全”→“IP过滤”选项，在右侧显示“IP过

滤”窗格，如下图所示，通过单击右侧窗格的“添加”按钮，可以为远程服务器添加IP过滤策略，选择配置好的配置文件，单击“使用配置文件”按钮，可以使该项IP过滤策划生效。



6.4 使用QuickIP实现远程控制入侵系统

对于网络管理员来说，往往需要使用一台计算机对多台计算机进行管理，此时就需要用到多点远程控制技术，而QuickIP就是一款具有多点远程控制技术的工具。

实战6：安装QuickIP工具

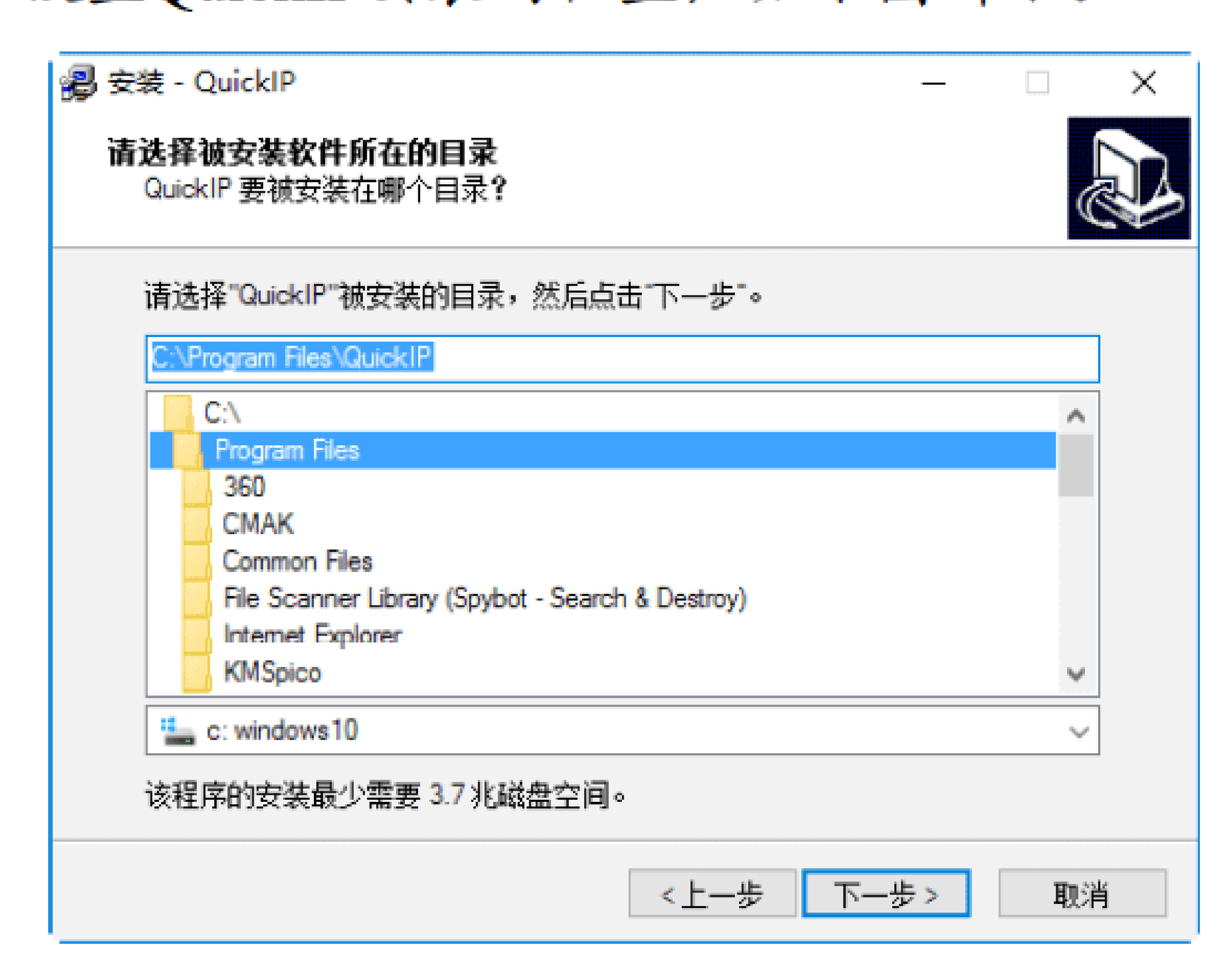
QuickIP是基于TCP/IP协议的一种工具，并且可运行在Windows的各种系统中，利用该工具可以全权控制远程的计算机。另外，该工具具有功能强大、使用简单等优点。

安装QuickIP的操作步骤如下。

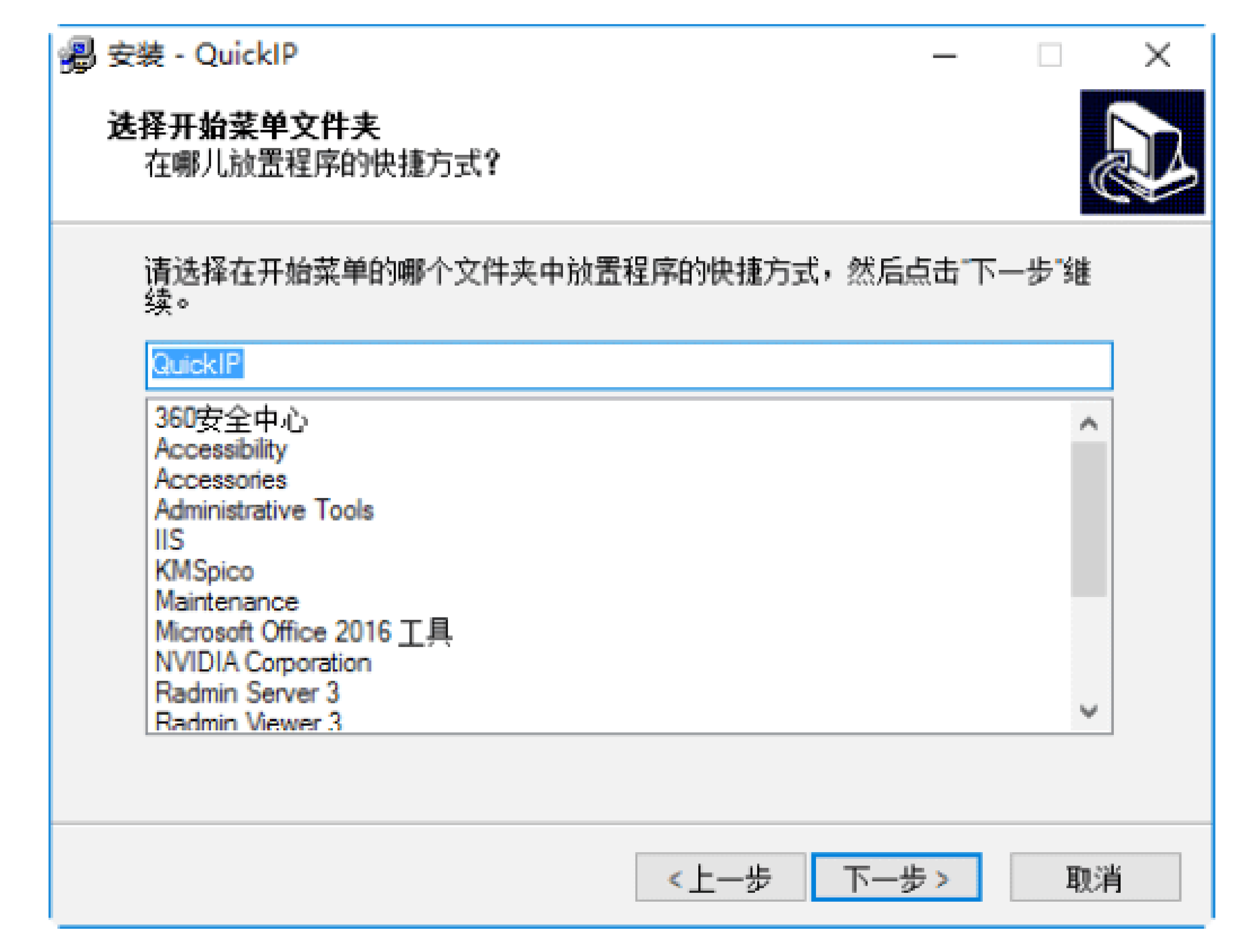
Step 01 双击QuickIP的安装程序，即可打开“欢迎使用QuickIP安装向导”对话框，如下图所示。



Step 02 单击“下一步”按钮，打开“请选择被安装软件所在的目录”对话框，在其中设置QuickIP安装的位置，如下图所示。

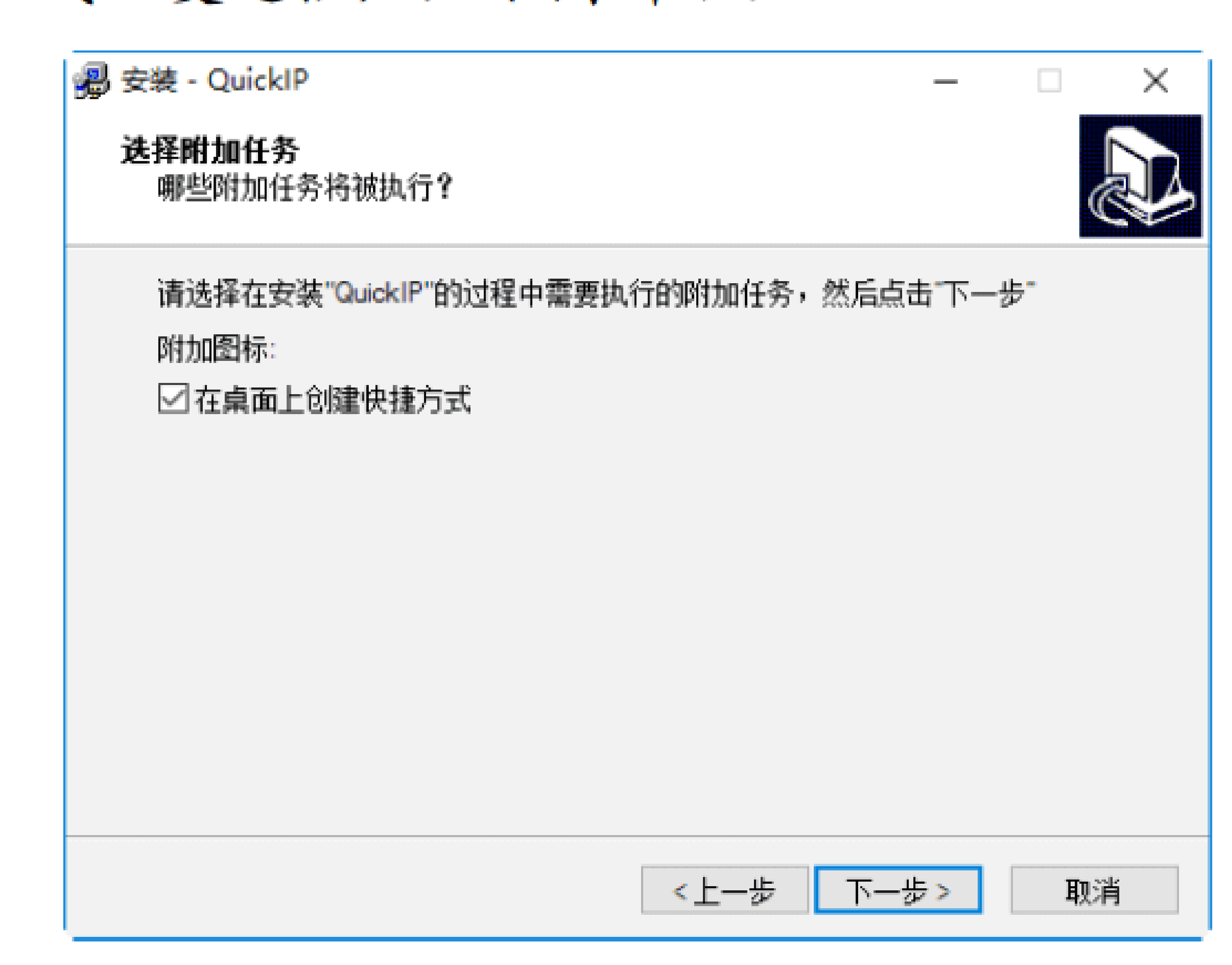


Step 03 单击“下一步”按钮，打开“选择开始菜单文件夹”对话框，在其中设置程序快捷方式的存在位置，如下图所示。

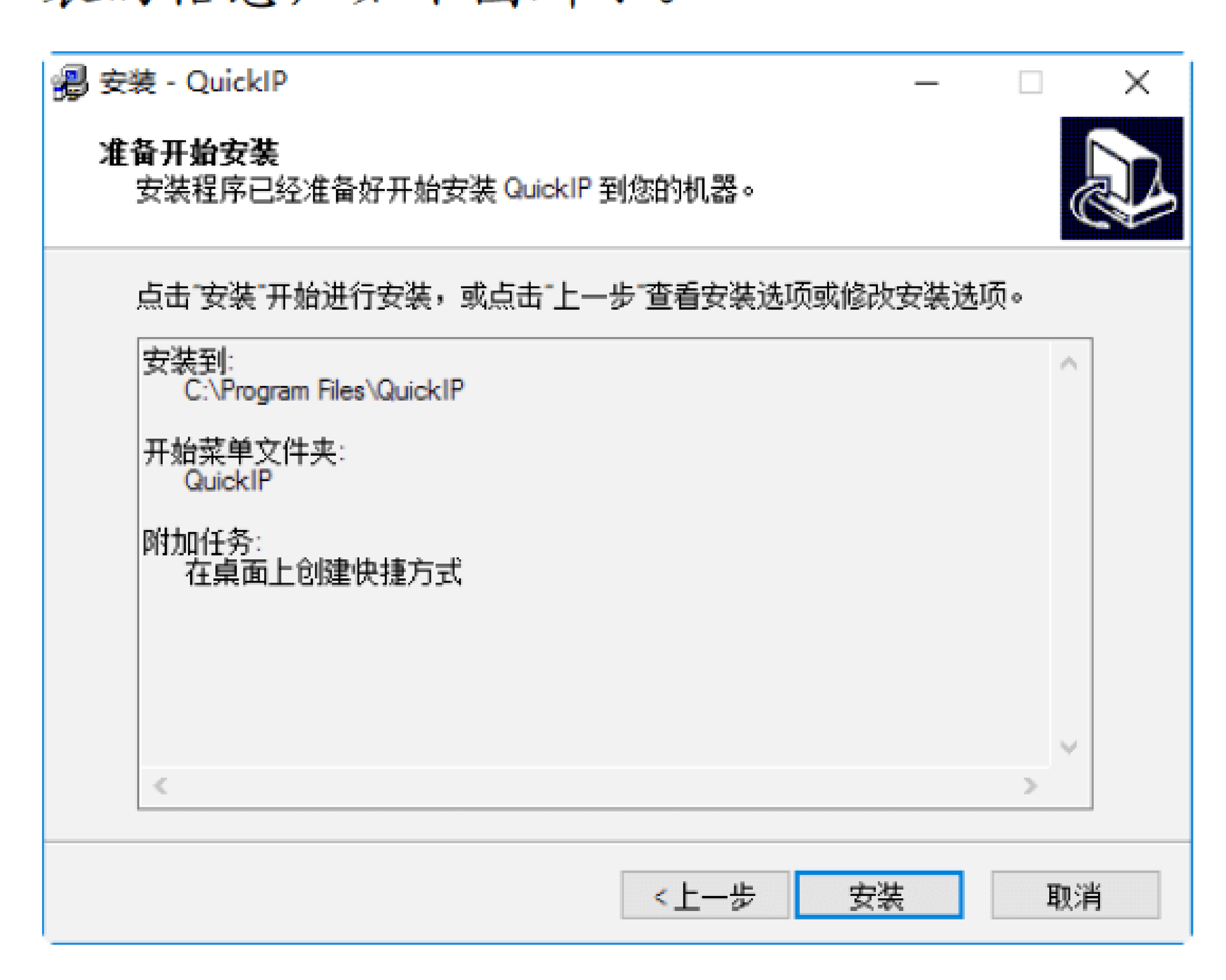




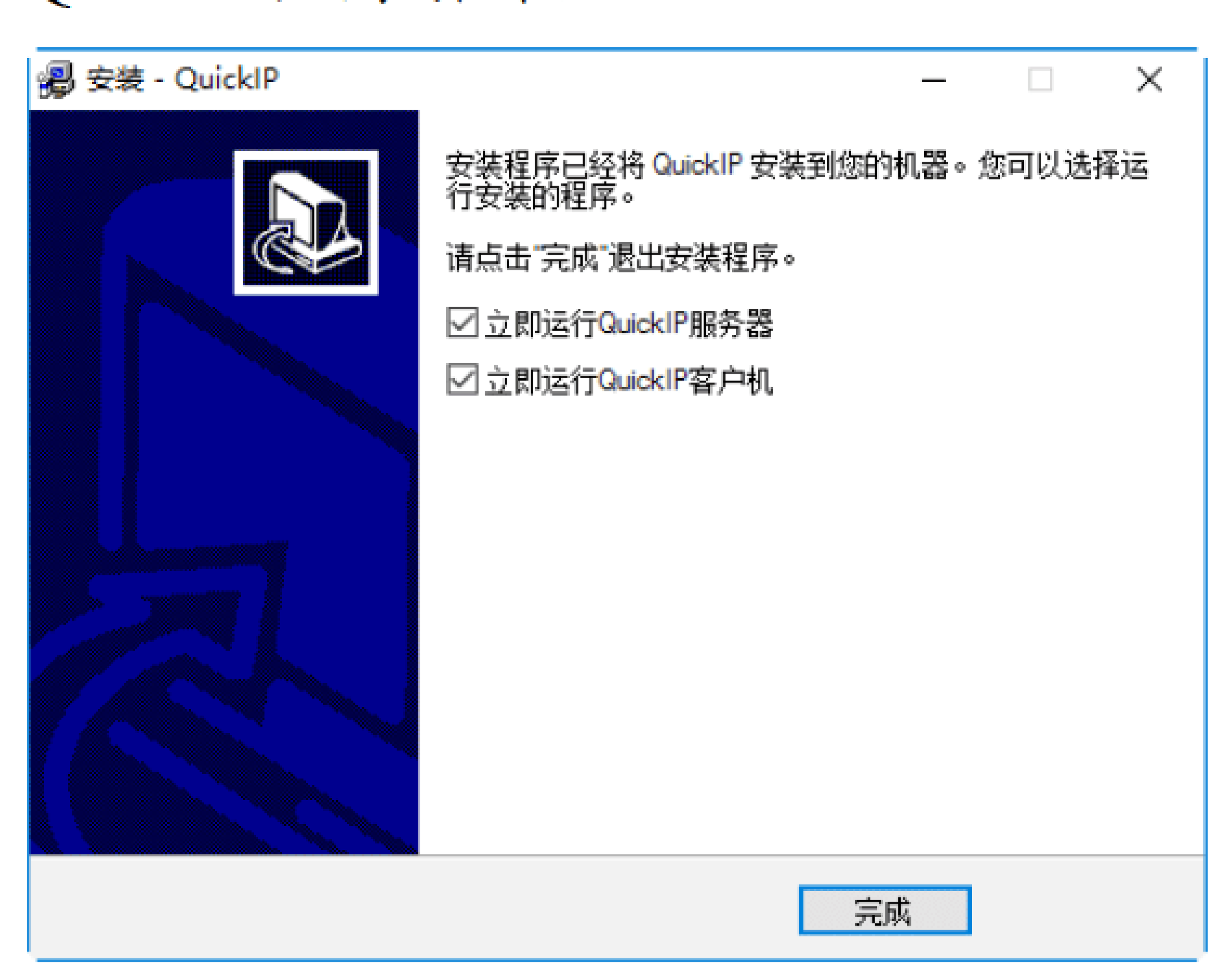
Step 04 单击“下一步”按钮，打开“选择附加任务”对话框，在其中设置被执行的附加任务，这里勾选“在桌面上创建快捷方式”复选框，如下图所示。



Step 05 单击“下一步”按钮，打开“准备开始安装”对话框，在其中可以查看将被安装的信息，如下图所示。



Step 06 单击“安装”按钮，开始安装QuickIP，安装完成后，将弹出如下图所示对话框，单击“完成”按钮，即可完成QuickIP的安装操作。



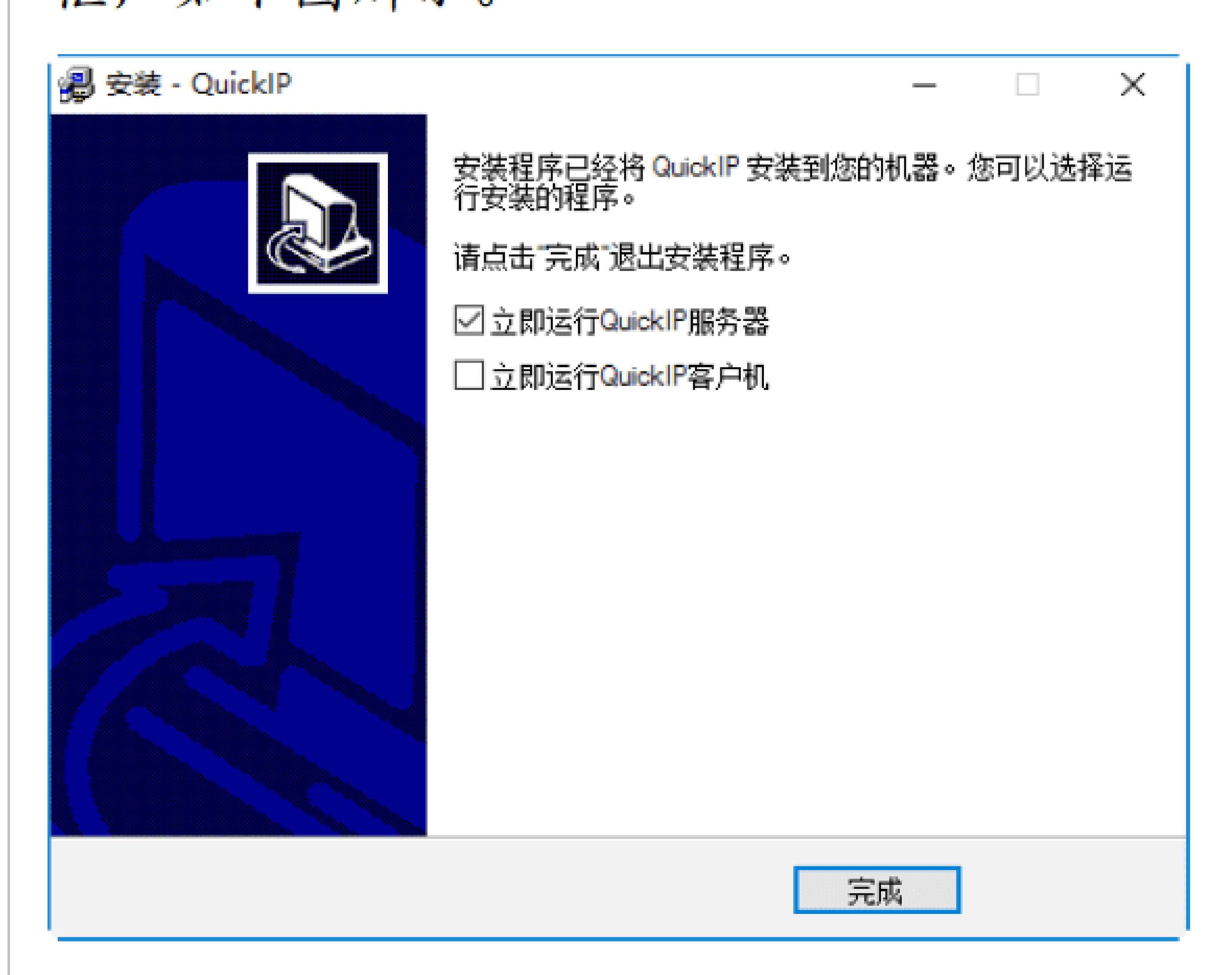


实战7：设置QuickIP服务端

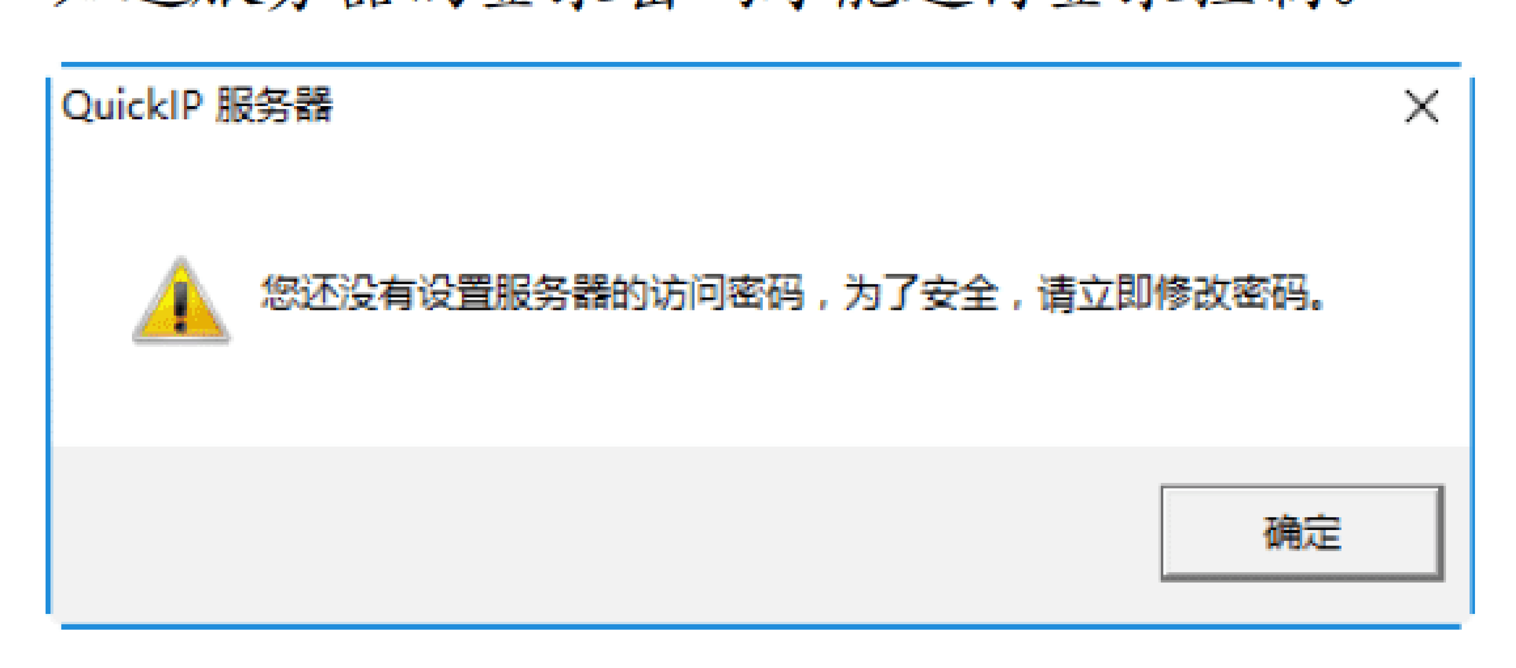
由于QuickIP工具是将服务器端与客户端合并在一起的，所以在计算机中都是服务器端和客户端一起安装的，这也是实现一台服务器可以同时被多个客户机控制、一个客户机也可以同时控制多个服务器的原因所在。

配置QuickIP服务器端的具体操作步骤如下。

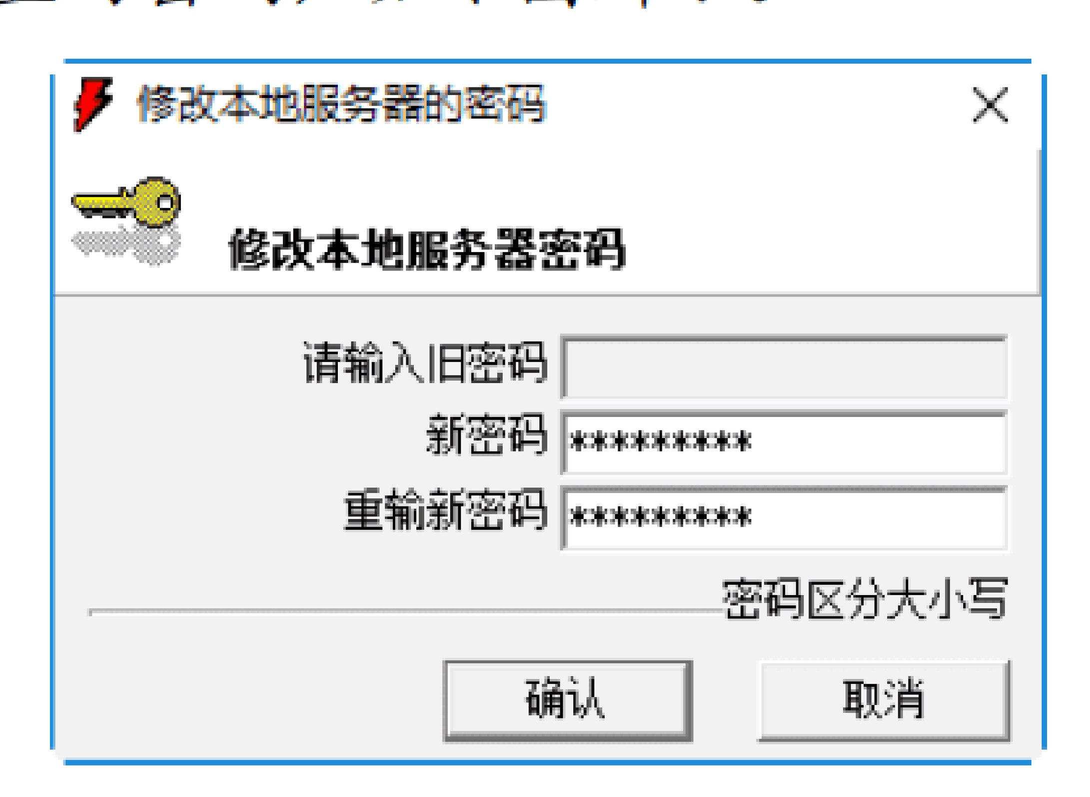
Step 01 QuickIP成功安装后，即可打开“QuickIP安装完成”对话框，在其中可以设置是否启动QuickIP客户机和服务器，在这里勾选“立即运行QuickIP服务器”复选框，如下图所示。



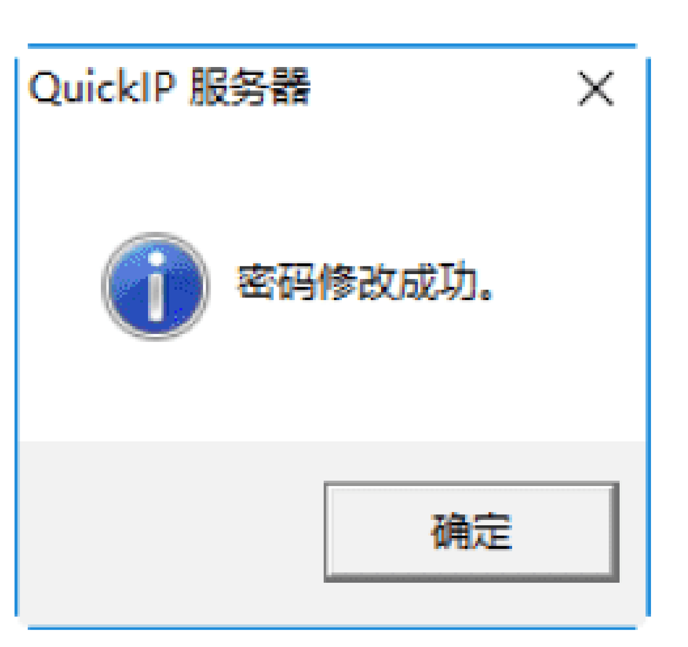
Step 02 单击“完成”按钮，即可打开“请立即修改密码”提示框，如下图所示，为了实现安全的密码验证登录，QuickIP设定客户端必须知道服务器的登录密码才能进行登录控制。



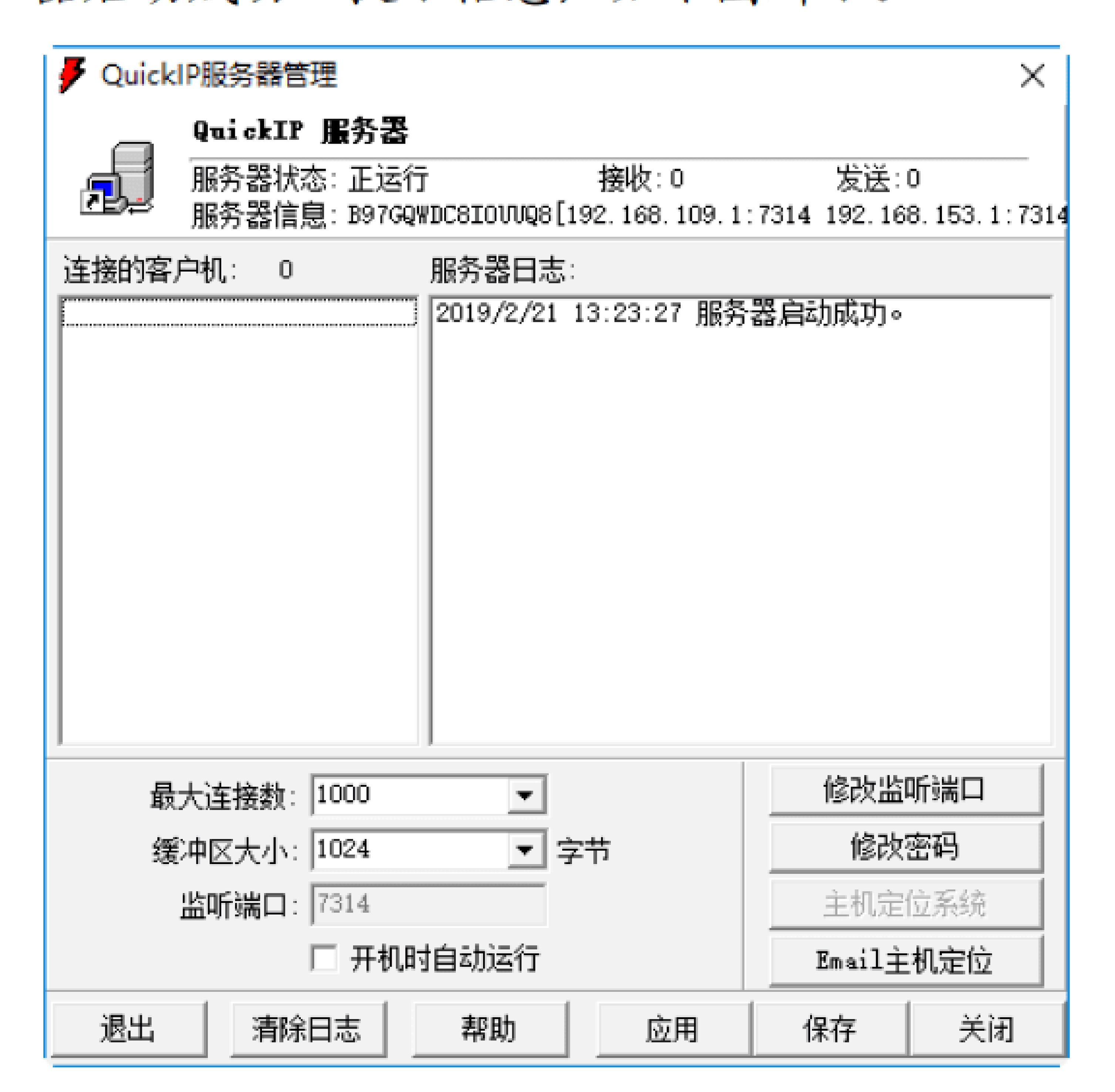
Step 03 单击“确定”按钮，即可打开“修改本地服务器的密码”对话框，在其中输入要设置的密码，如下图所示。



Step 04 单击“确认”按钮，即可看到“密码修改成功”提示框，如下图所示。



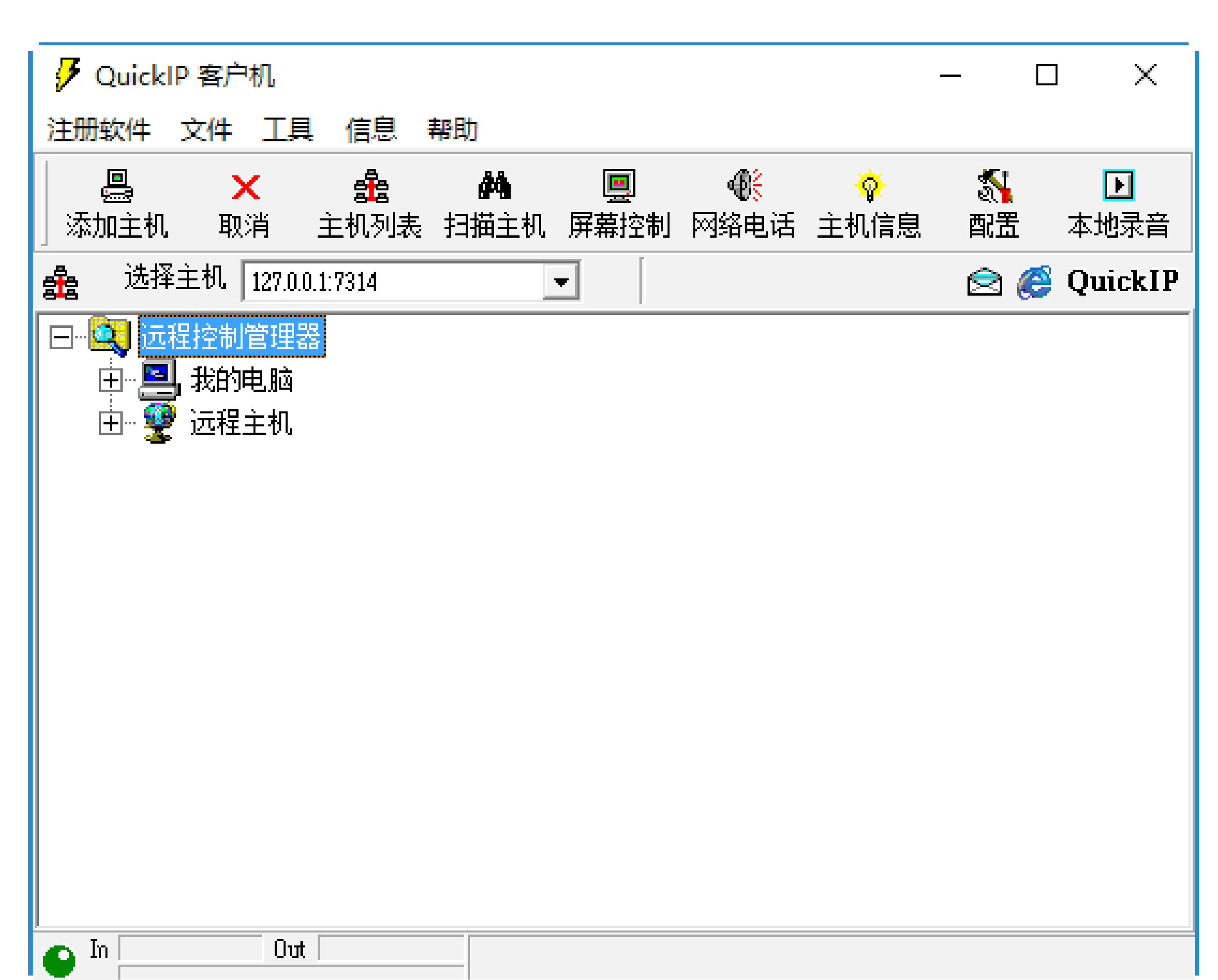
Step 05 单击“确定”按钮，即可打开“QuickIP服务器管理”对话框，在其中即可看到“服务器启动成功”提示信息，如下图所示。



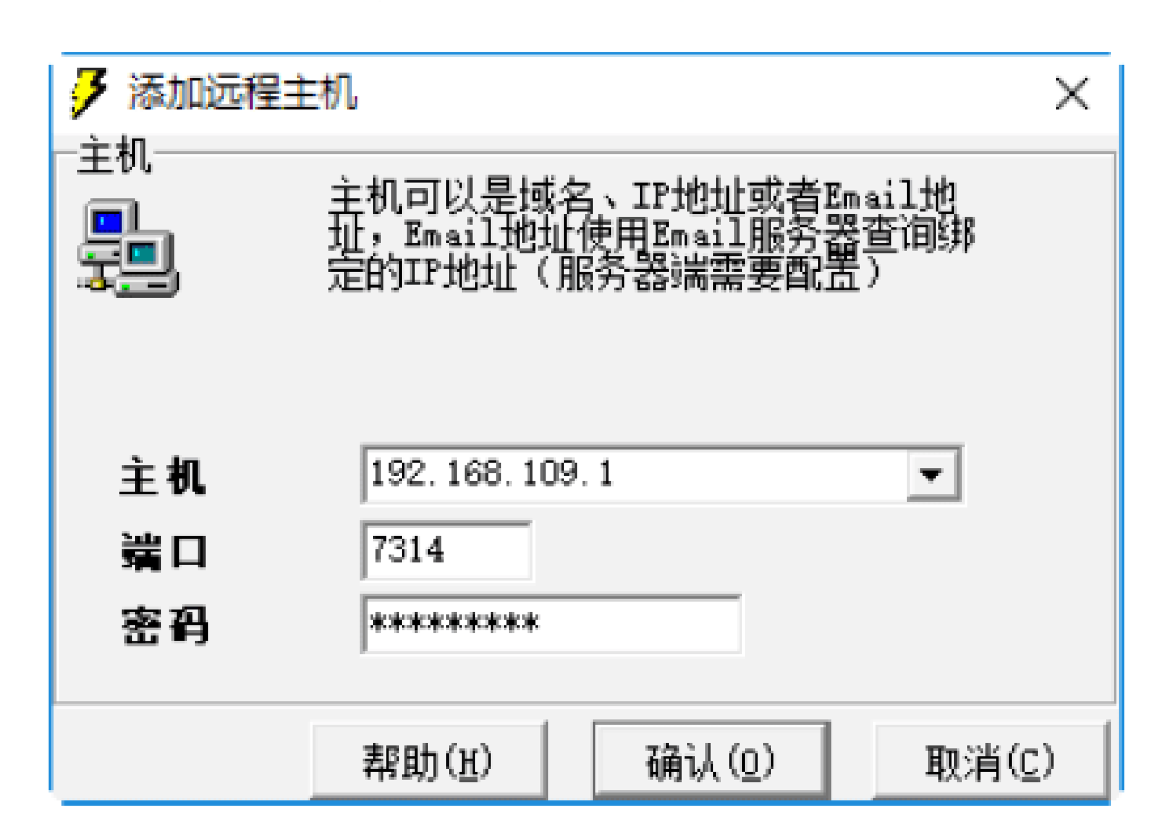
实战8：设置QuickIP客户端

在设置完服务端之后，就需要设置QuickIP客户端。设置客户端相对比较简单，主要是在客户端中添加远程主机。具体操作步骤如下。

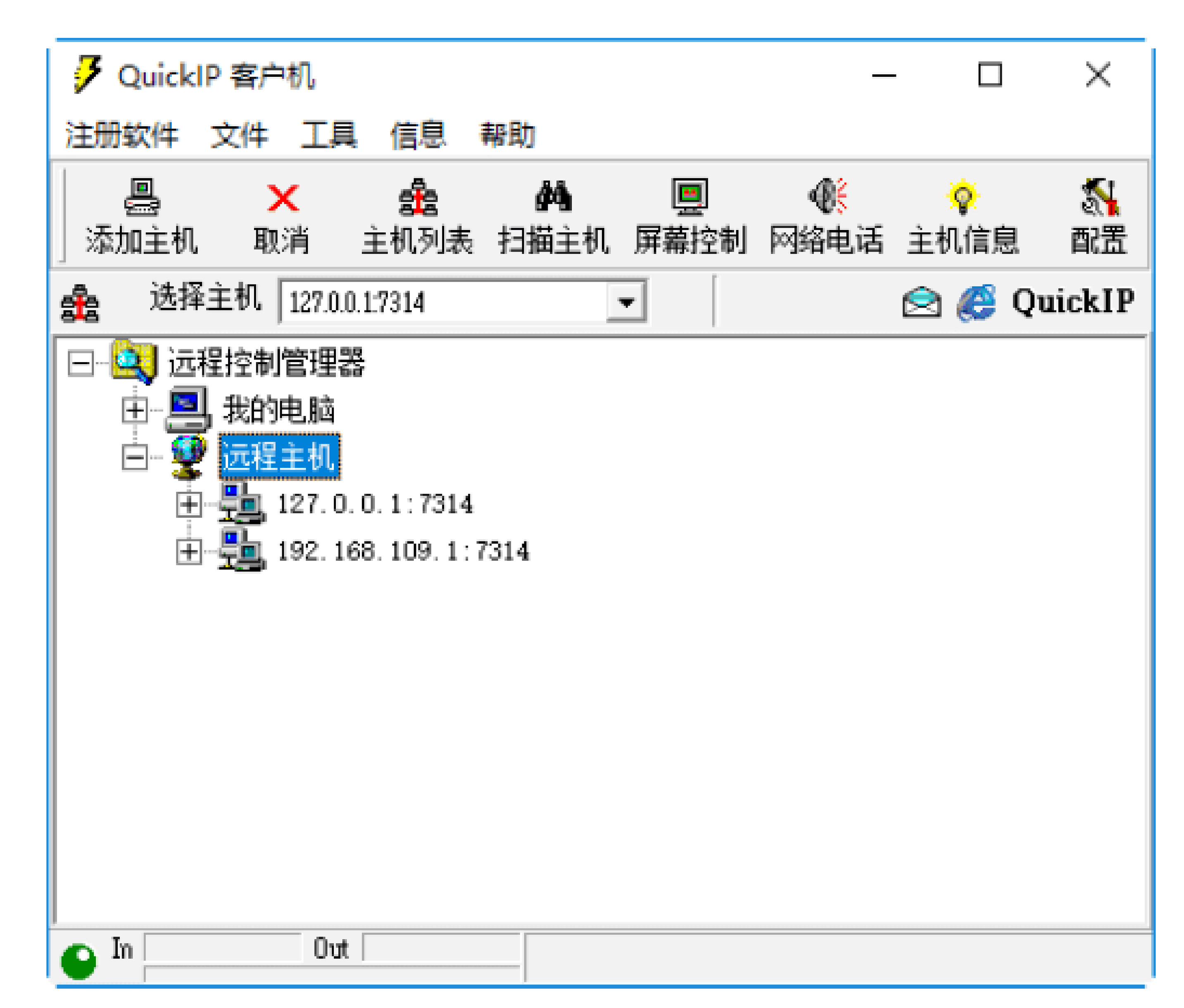
Step 01 选择“开始”→“所有应用”→QuickIP→“QuickIP客户机”选项，即可打开“QuickIP客户机”主窗口，如下图所示。



Step 02 单击工具栏中的“添加主机”按钮，打开“添加远程主机”对话框。在“主机”文本框中输入远程计算机的IP地址，在“端口”和“密码”文本框中输入在服务器端设置的信息，如下图所示。

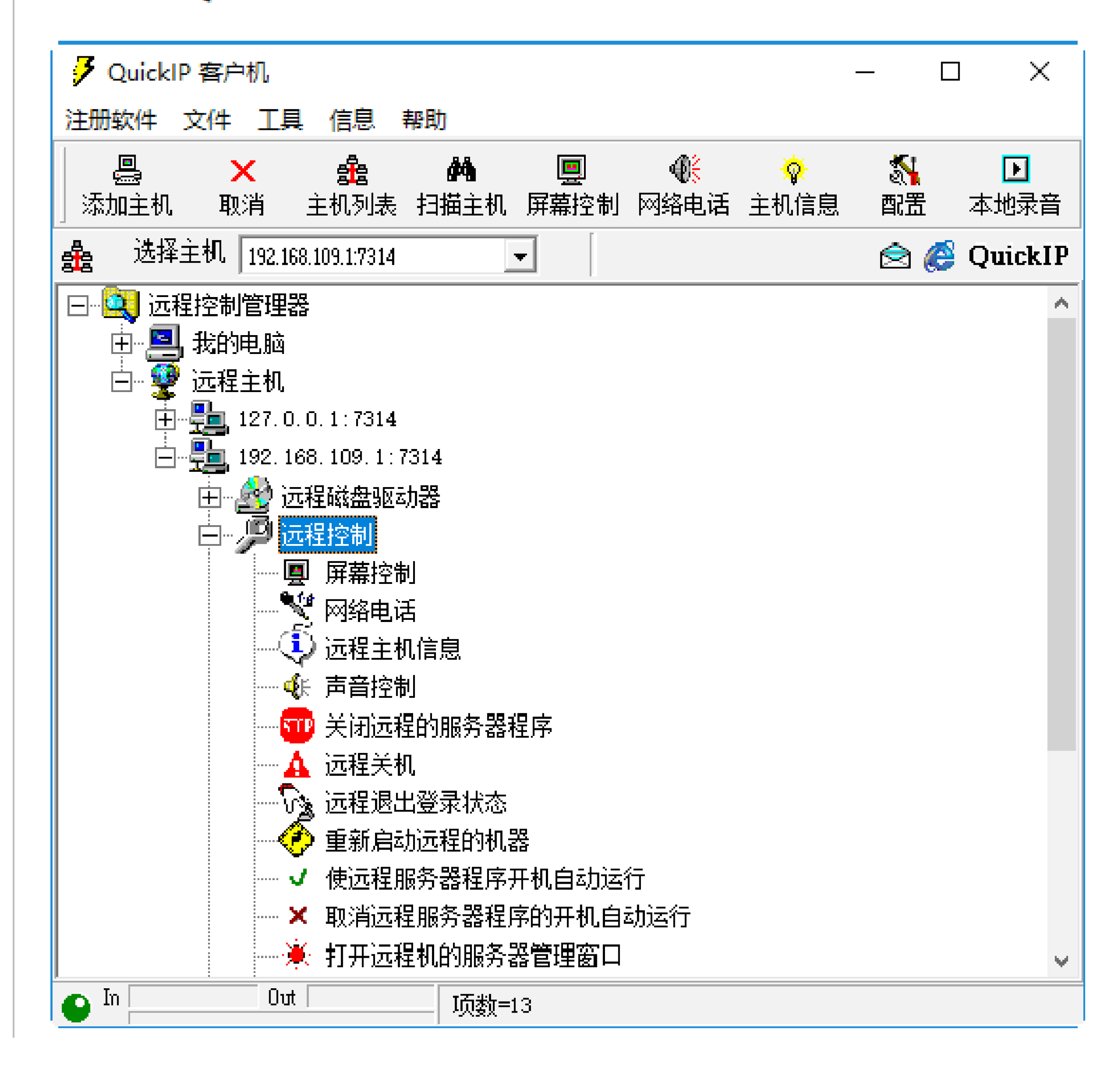


Step 03 单击“确定”按钮，即可在“QuickIP客户机”主窗口中的“远程主机”下看到刚刚添加的IP地址，如下图所示。





Step 04 单击该IP地址，从展开的控制功能列表中可看到远程控制功能十分丰富，如下图所示，这表示客户端与服务器端的连接已经成功。



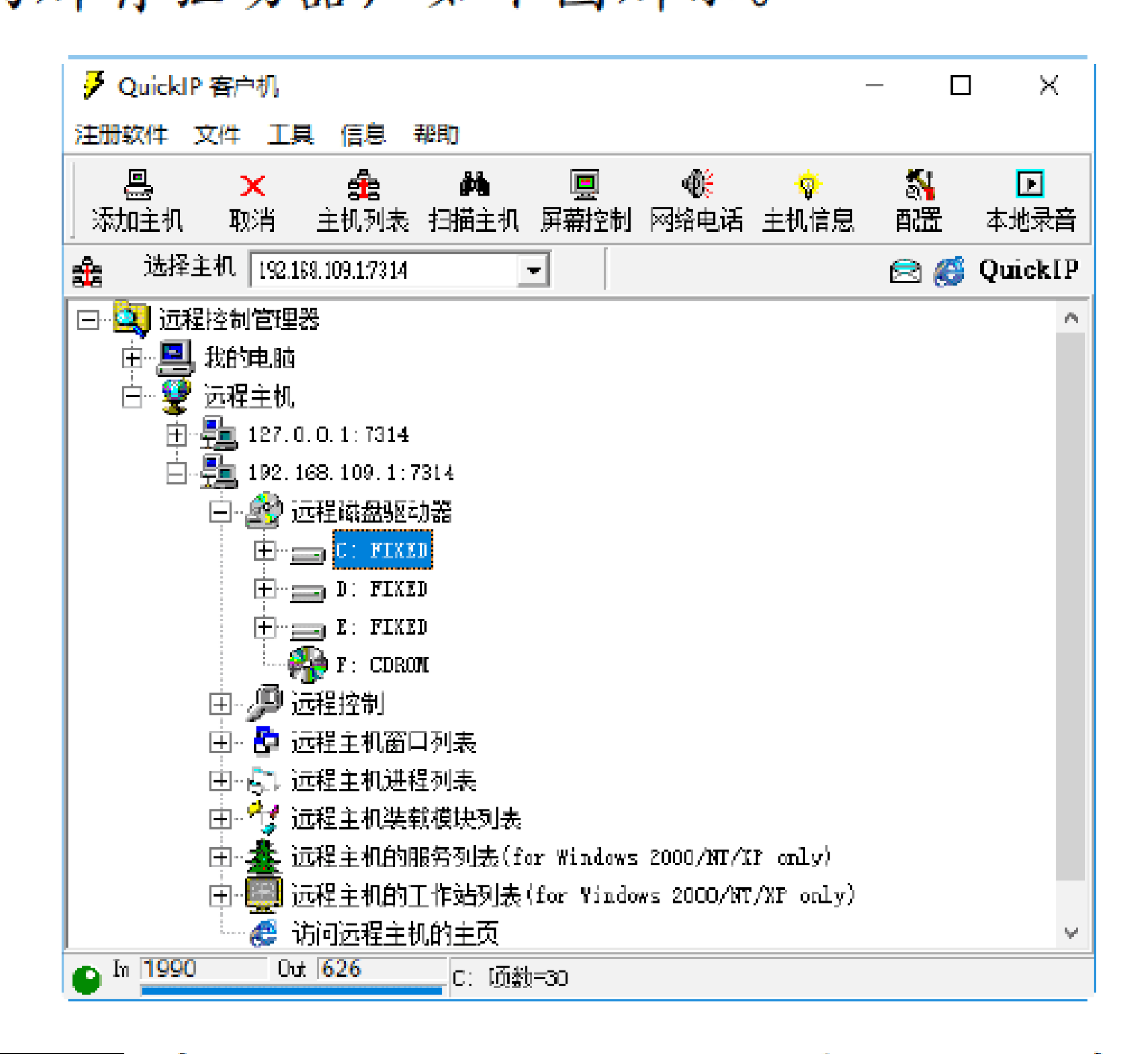
实战9：实现远程控制入侵

在成功添加远程主机之后，就可以利用QuickIP工具对其进行远程控制。由于Quick-IP功能非常强大，这里只介绍几个常用的功能。实现远程控制的具体步骤如下。

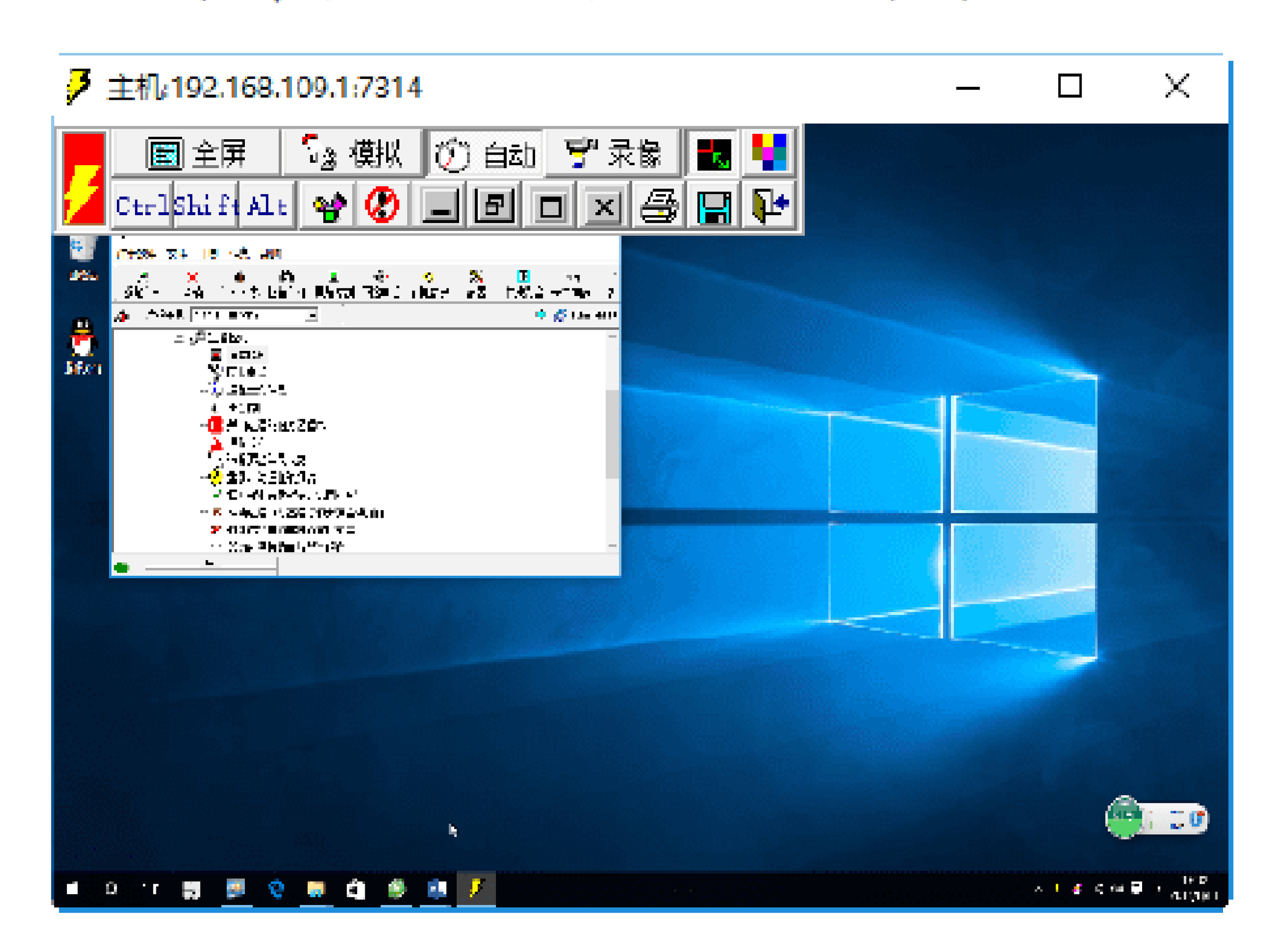
Step 01 在“192.168.109.1：7314”栏目下单击“远程磁盘驱动器”选项，即可打开“登录到远程主机”对话框，如下图所示。



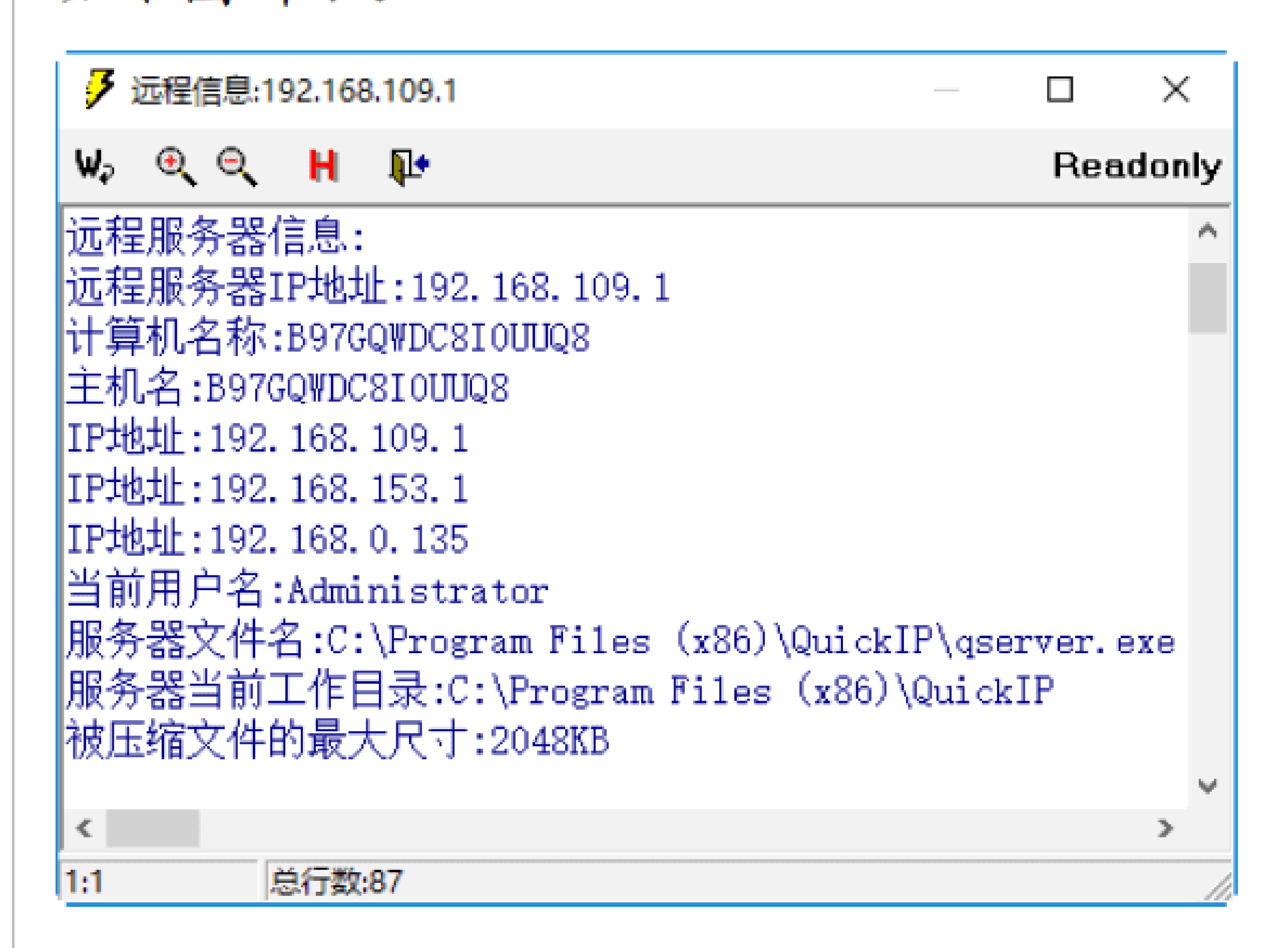
Step 02 在其中输入设置的端口和密码后，单击“确认”按钮，即可看到远程计算机中的所有驱动器，如下图所示。



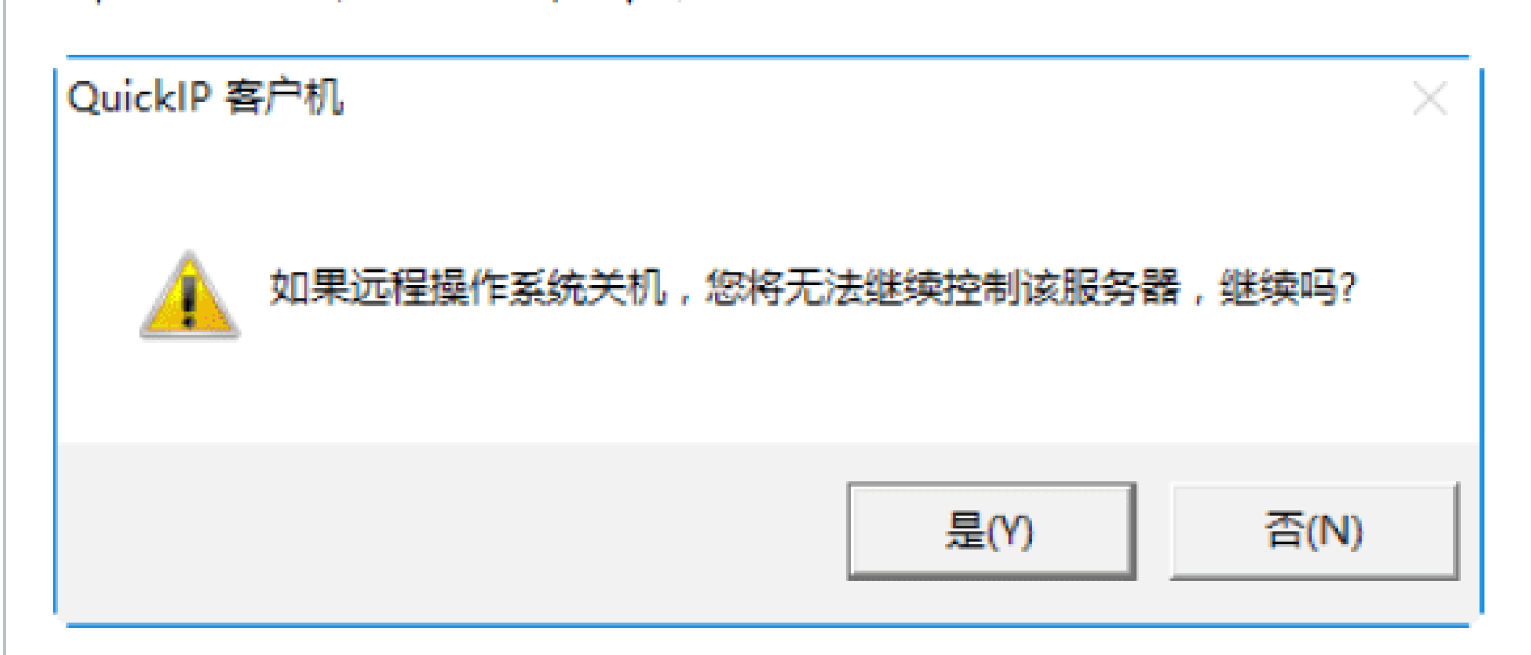
Step 03 单击“远程控制”选项中的“屏幕控制”子项，稍等片刻，即可看到远程计算机的桌面，在其中可通过鼠标和键盘完成对远程计算机的控制，如下图所示。



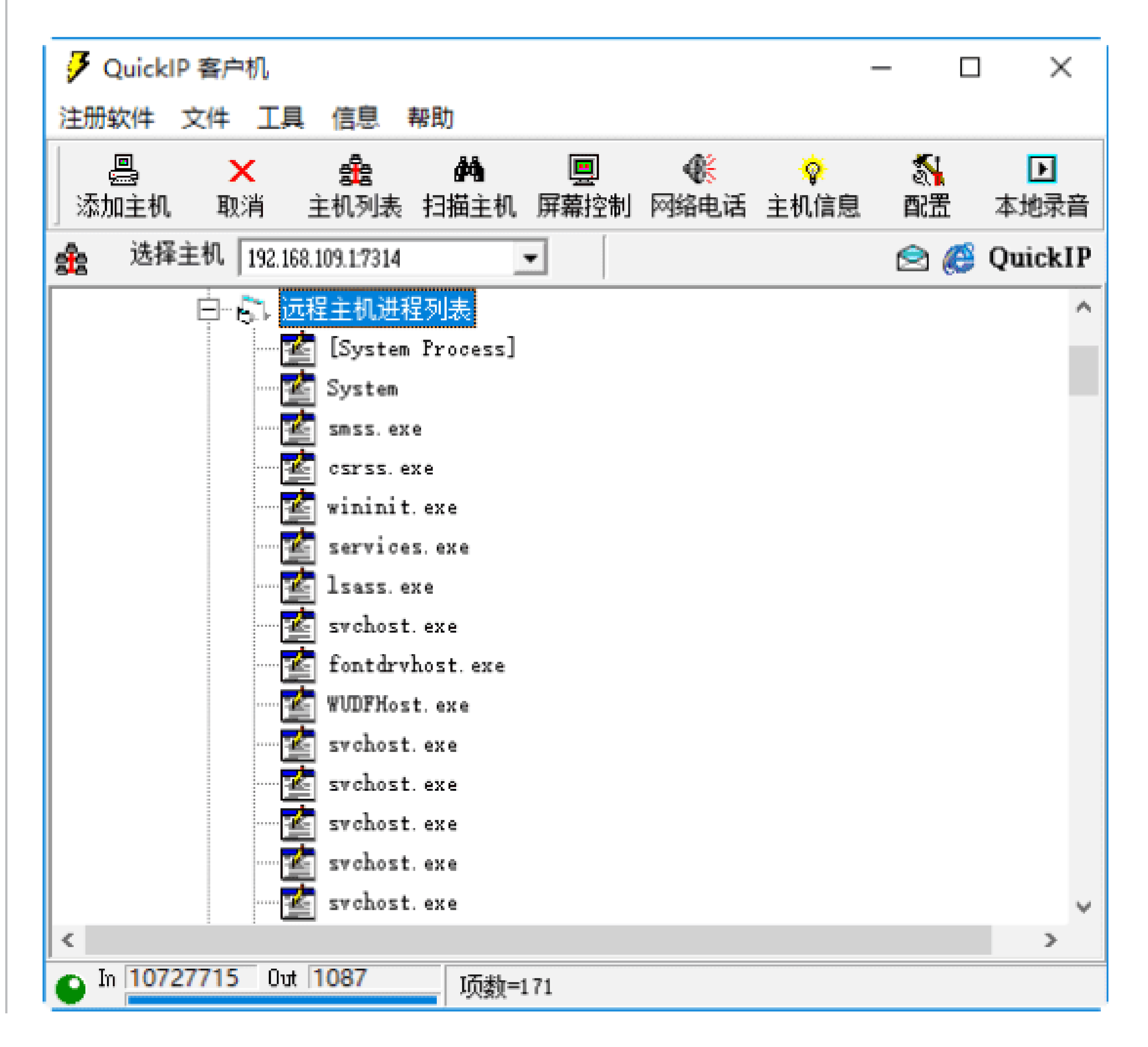
Step 04 单击“远程控制”选项中的“远程主机信息”子项，即可打开“远程信息”窗口，在其中即可看到远程主机的详细信息，如下图所示。



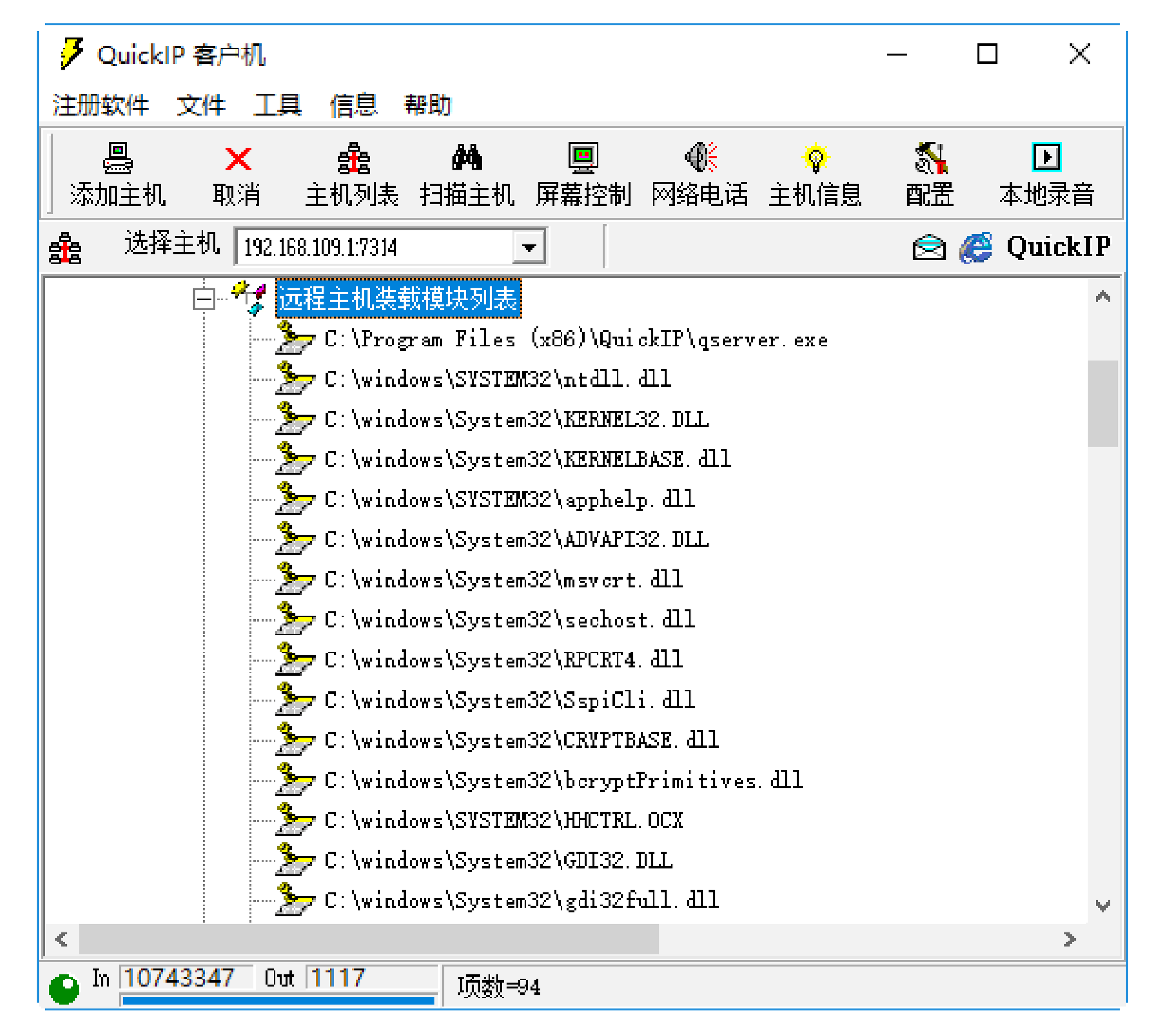
Step 05 如果要结束对远程计算机的操作，为了安全起见，就应该关闭远程计算机。单击“远程控制”选项中的“远程关机”子项，即可打开“是否继续控制该服务器”对话框，如下图所示。单击“是”按钮，即可关闭远程计算机。



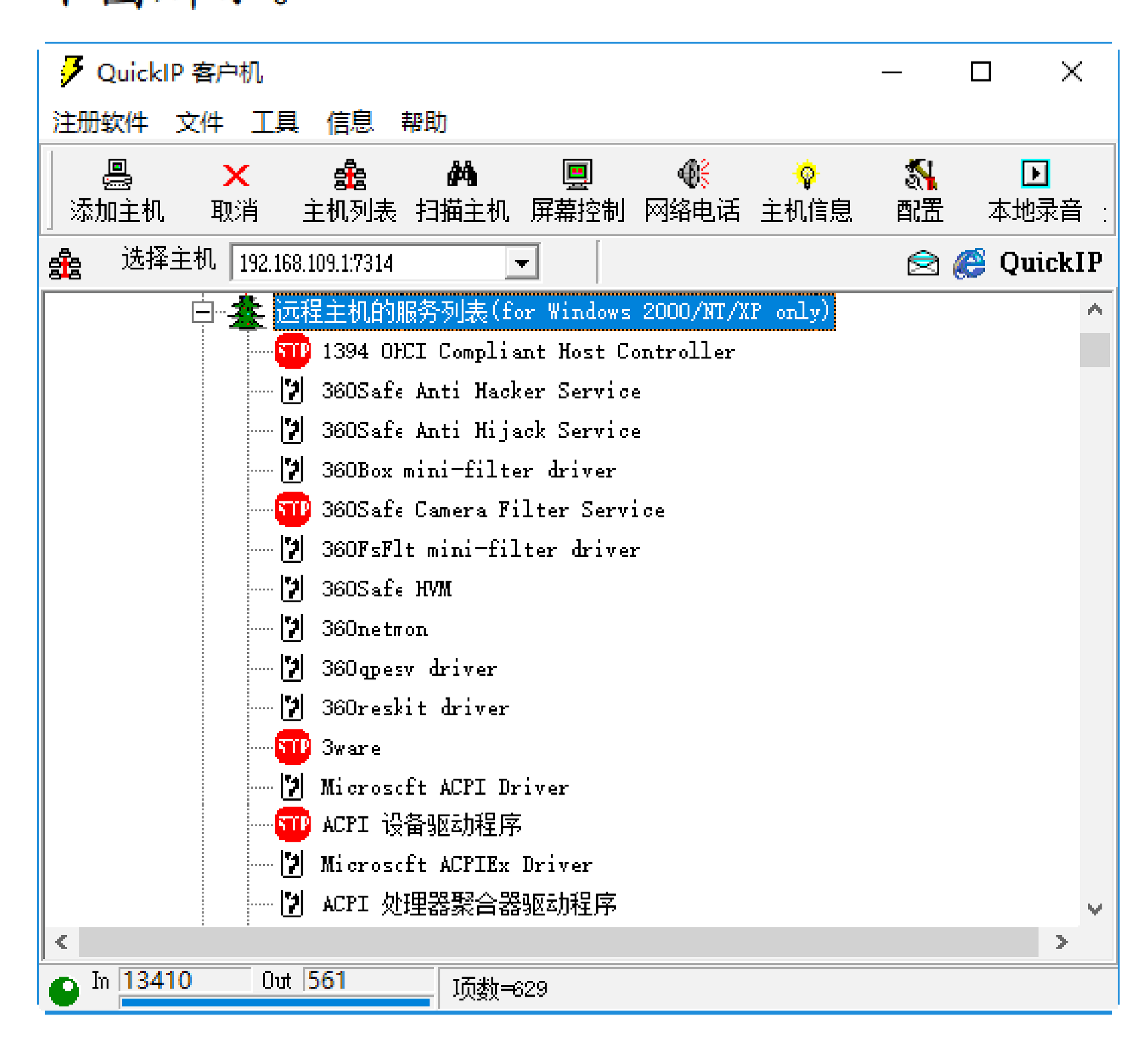
Step 06 在“192.168.109.1:7314”栏目下单击“远程主机进程列表”选项，在其中即可看到远程计算机中正在运行的进程，如下图所示。



Step 07 在“192.168.109.1:7314”栏目下单击“远程主机装载模块列表”选项，在其中即可看到远程计算机中装载模块列表，如下图所示。



Step 08 在“192.168.109.1:7314”栏目下单击“远程主机的服务列表”选项，在其中即可看到远程计算机中正在运行的服务，如下图所示。



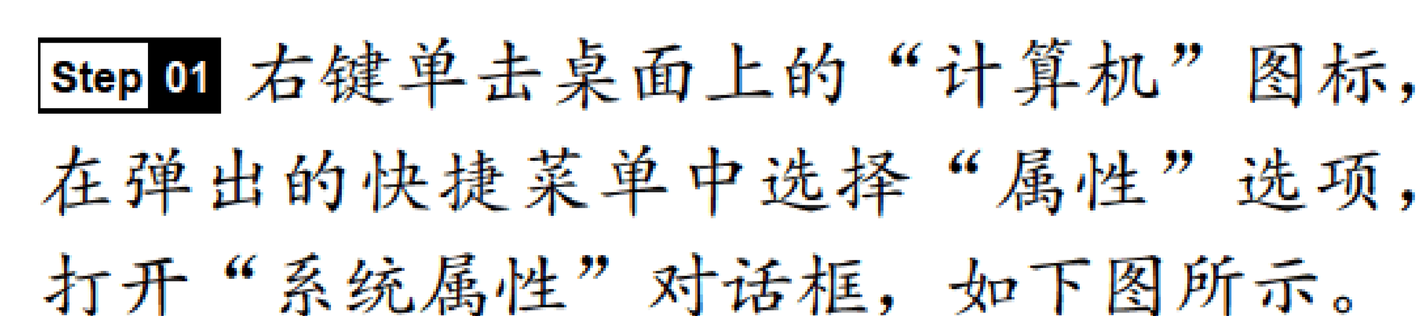
6.5　远程控制入侵系统的安全防护策略

要想使自己的计算机不受远程控制入侵的困扰，就需要用户对自己的计算机进行相应的保护操作，如关闭自己计算机的远程控制功能、安装相应的防火墙等。

实战10：关闭Window远程桌面功能



关闭Window远程桌面功能是防止黑客远程入侵系统的首要工作。具体的操作步骤如下。



Step 01 右键单击桌面上的“计算机”图标，在弹出的快捷菜单中选择“属性”选项，打开“系统属性”对话框，如下图所示。



Step 02 取消勾选“允许远程协助连接这台计算机”复选框，选中“不允许远程连接到此计算机”单选按钮，如下图所示，然后单击“确定”按钮，即可关闭Windows系统的远程桌面功能。



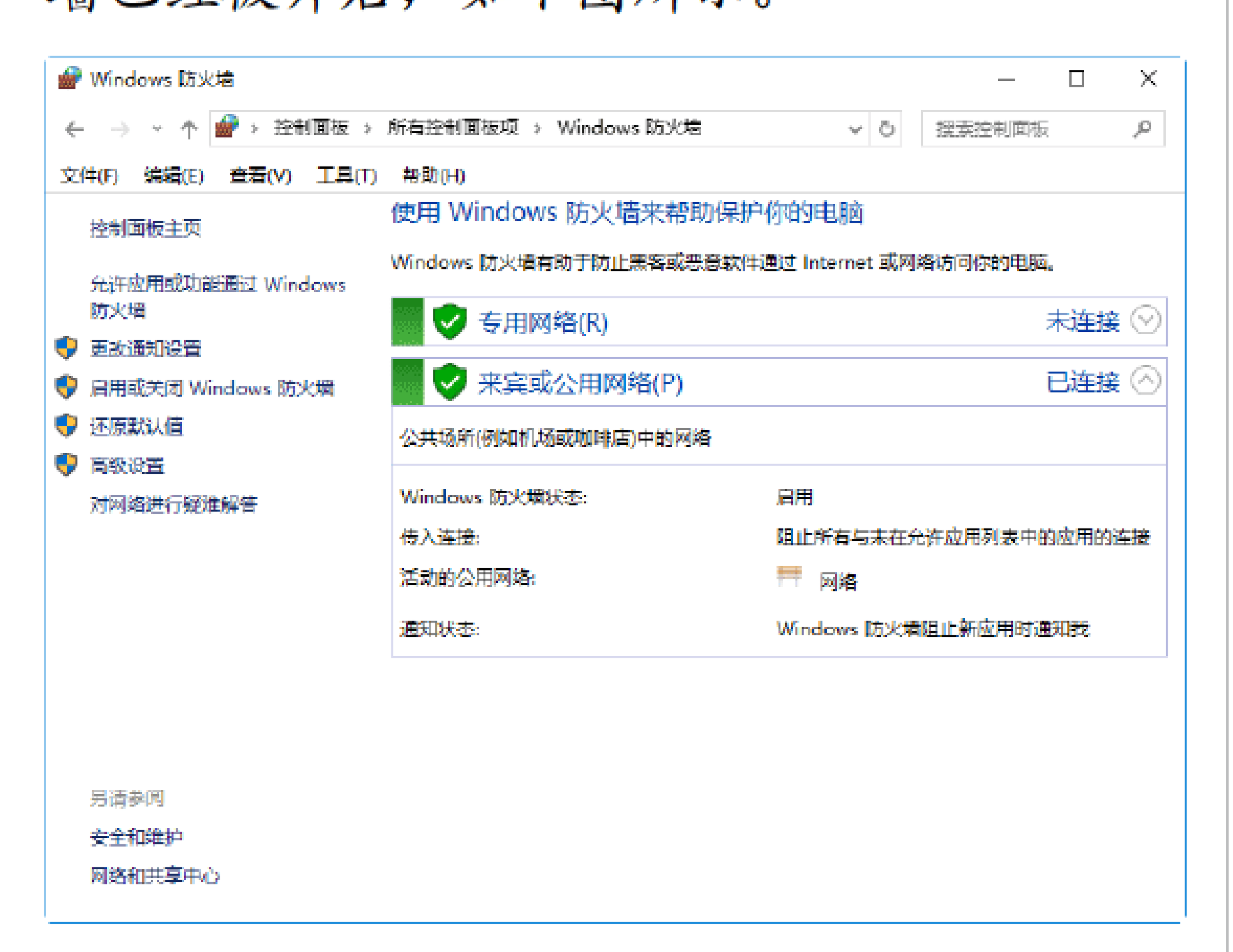


实战11：开启拒绝系统入侵的防火墙

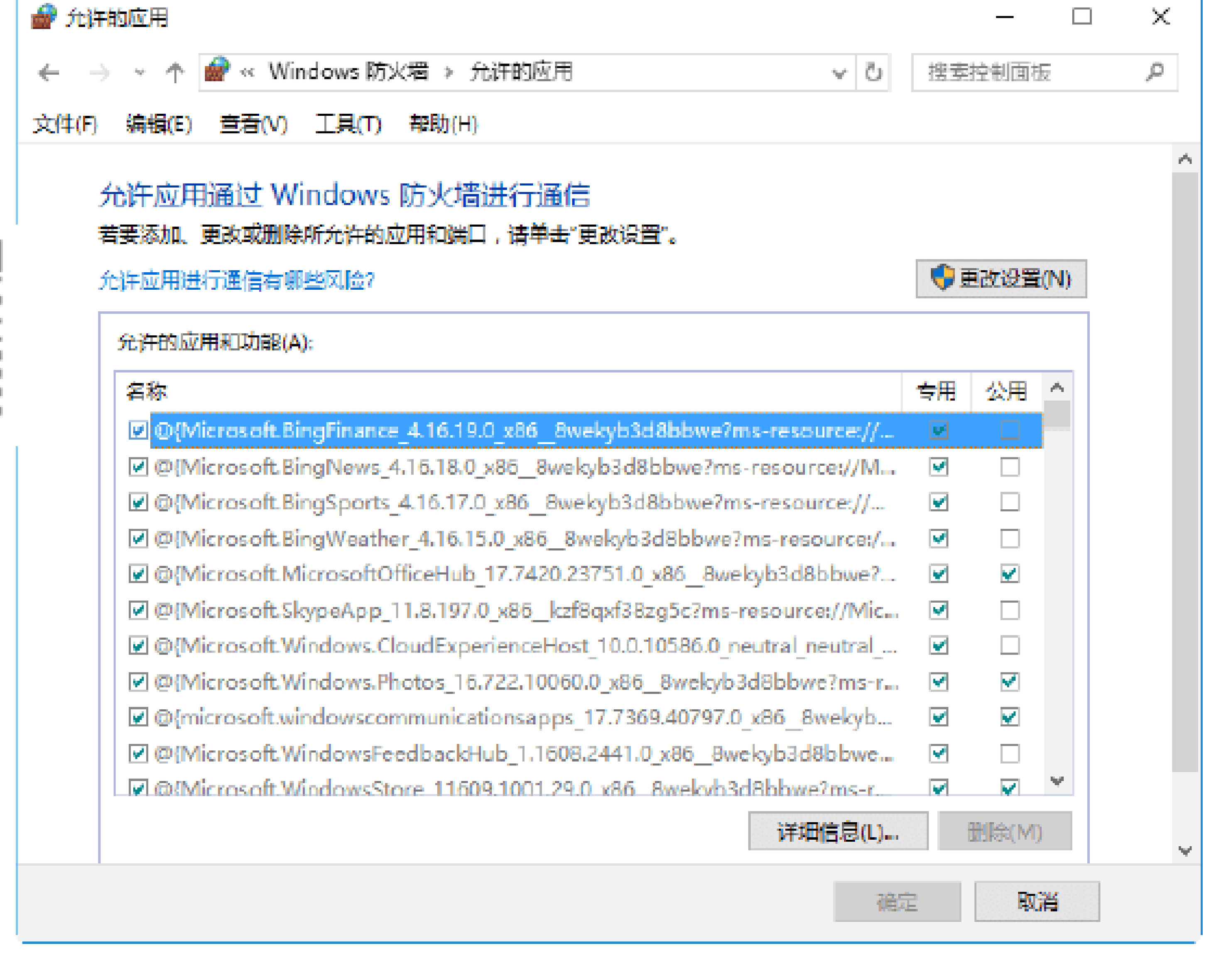
为了更好地进行网络安全管理，Windows系统特意为用户提供了防火墙功能。如果能够巧妙地使用该功能，就可以根据实际需要允许或拒绝网络信息通过，从而达到防范攻击、保护系统安全的目的。

使用Windows自带防火墙的具体操作步骤如下。

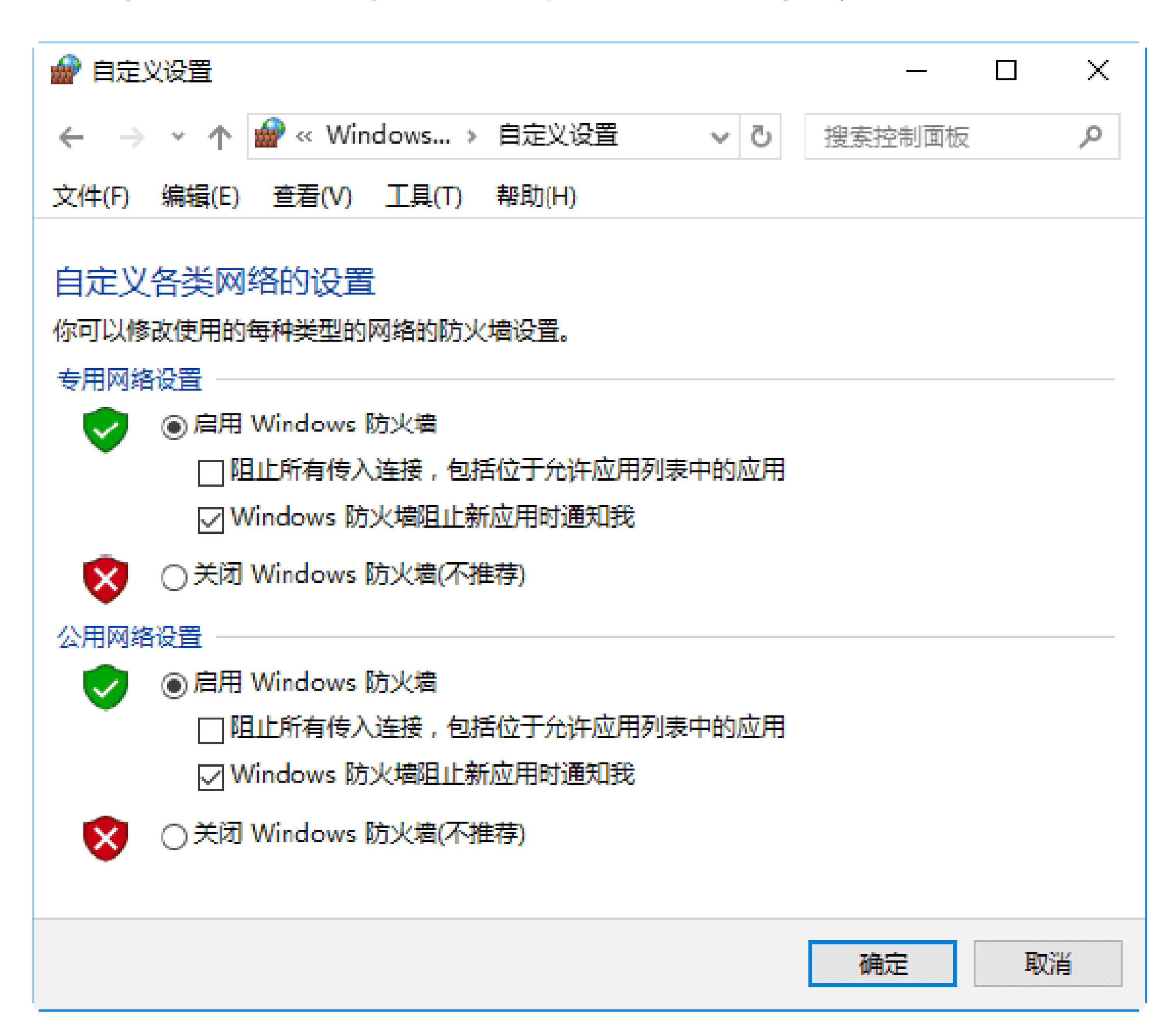
Step 01 在“控制面板”窗口中双击“Windows防火墙”图标项，打开“Windows防火墙”对话框，在对话框中显示此时Windows防火墙已经被开启，如下图所示。



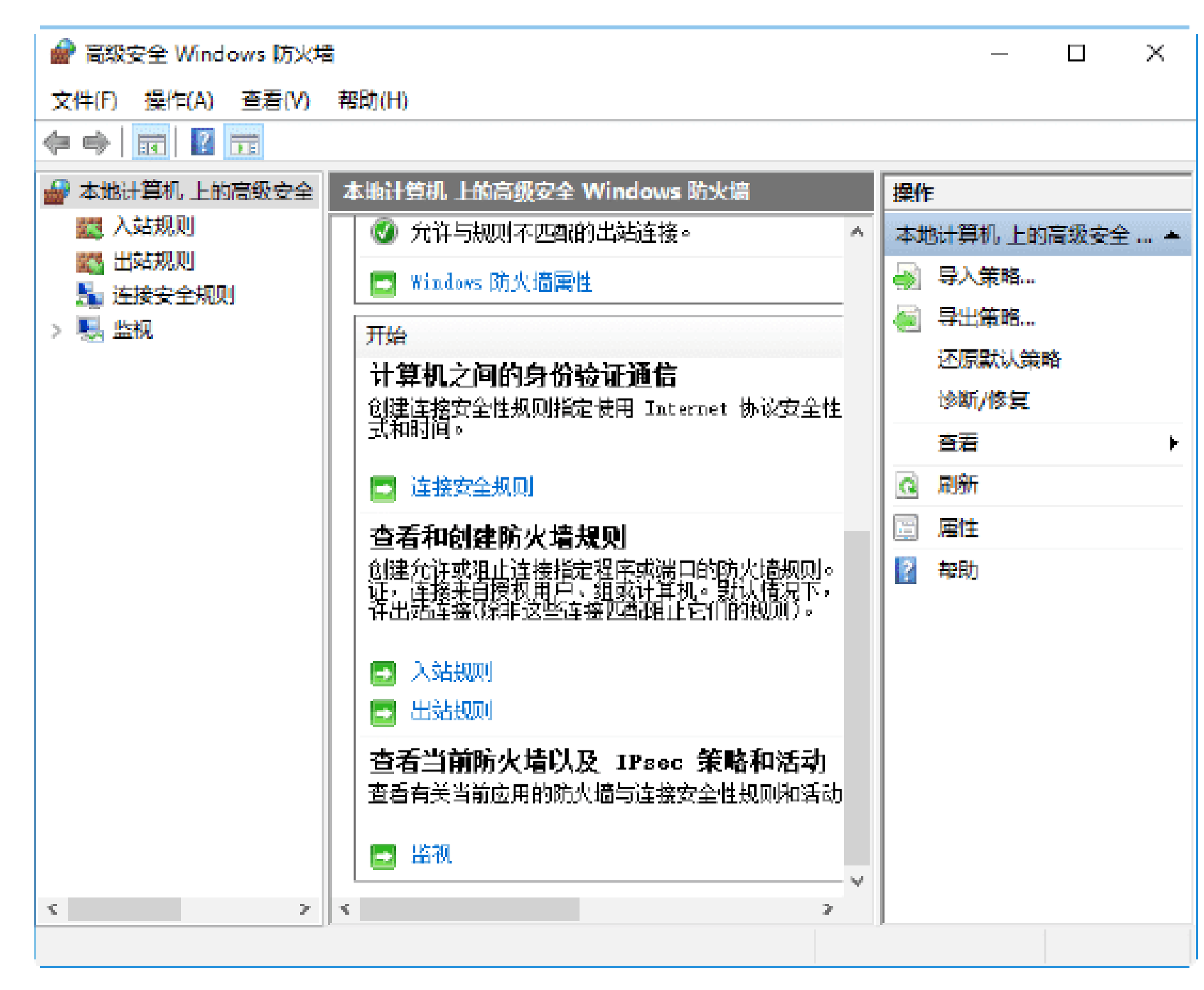
Step 02 单击“允许应用或功能通过Windows防火墙”链接，在打开的窗口中可以设置哪些程序或功能允许通过Windows防火墙访问外网，如下图所示。



Step 03 单击“更改通知设置”或“启用或关闭Windows防火墙”链接，打开的窗口中可以开启或关闭防火墙，如下图所示。



Step 04 单击“高级设置”链接，进入“高级设置”窗口，在其中可以对入站、出站、连接安全等规则进行设定，如下图所示。

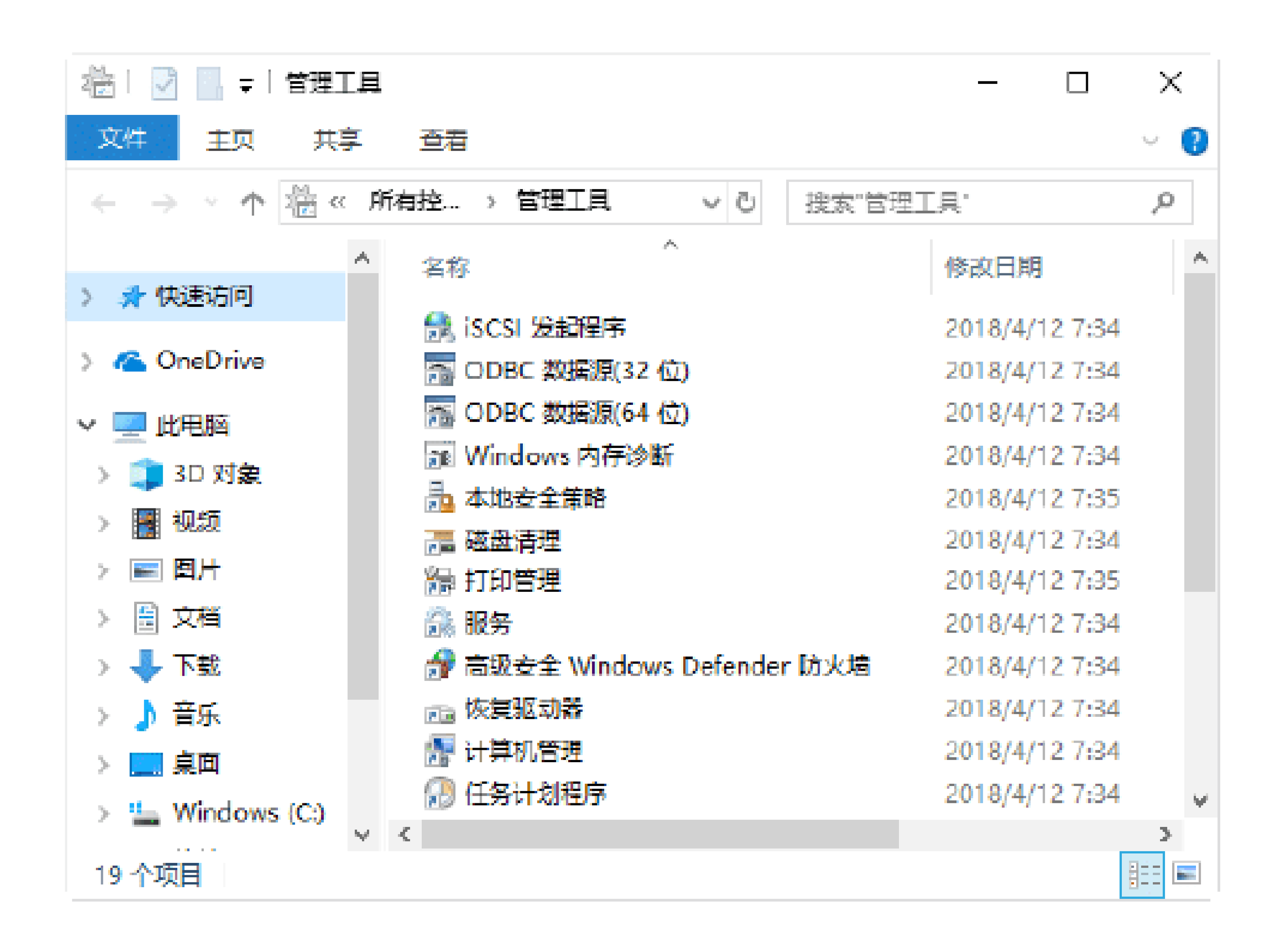


实战12：关闭远程注册表管理服务

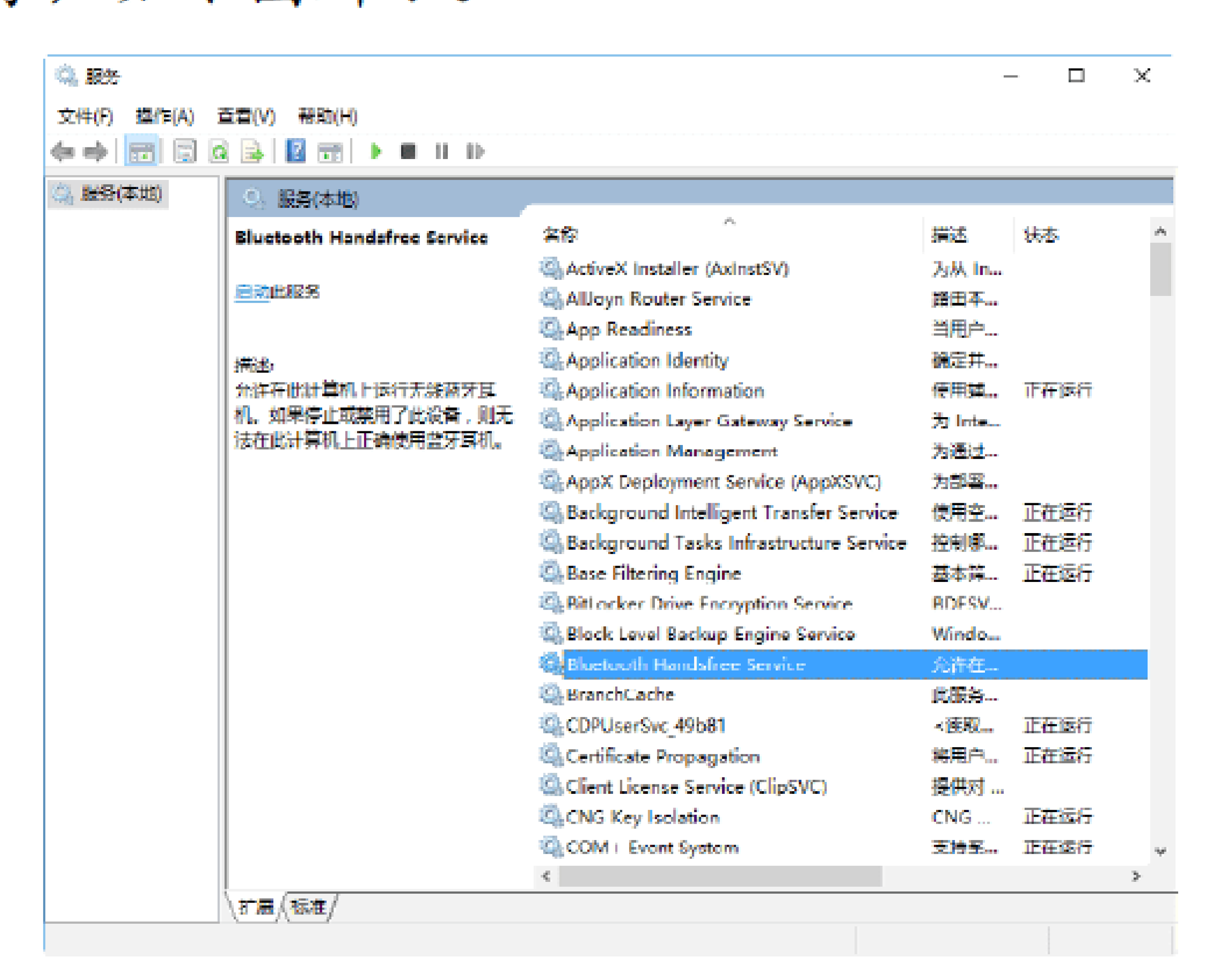
远程控制注册表主要是为了方便网络管理员对网络中的计算机进行管理，但这样却给黑客入侵提供了方便。因此，必须关闭远程注册表管理服务。具体的操作步骤如下。

Step 01 在“控制面板”窗口中双击“管理工具”选项，进入“管理工具”窗口，如下图所示。

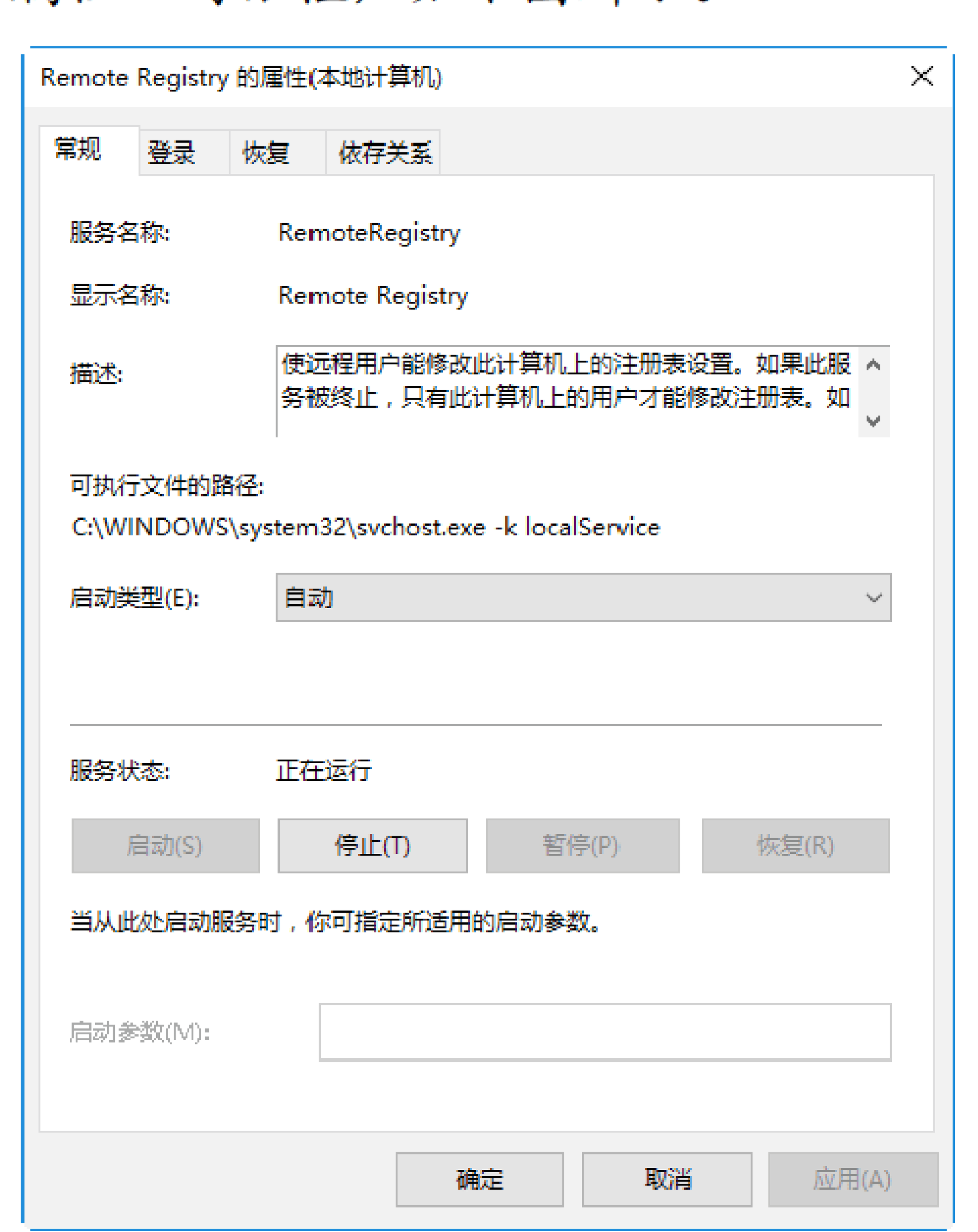




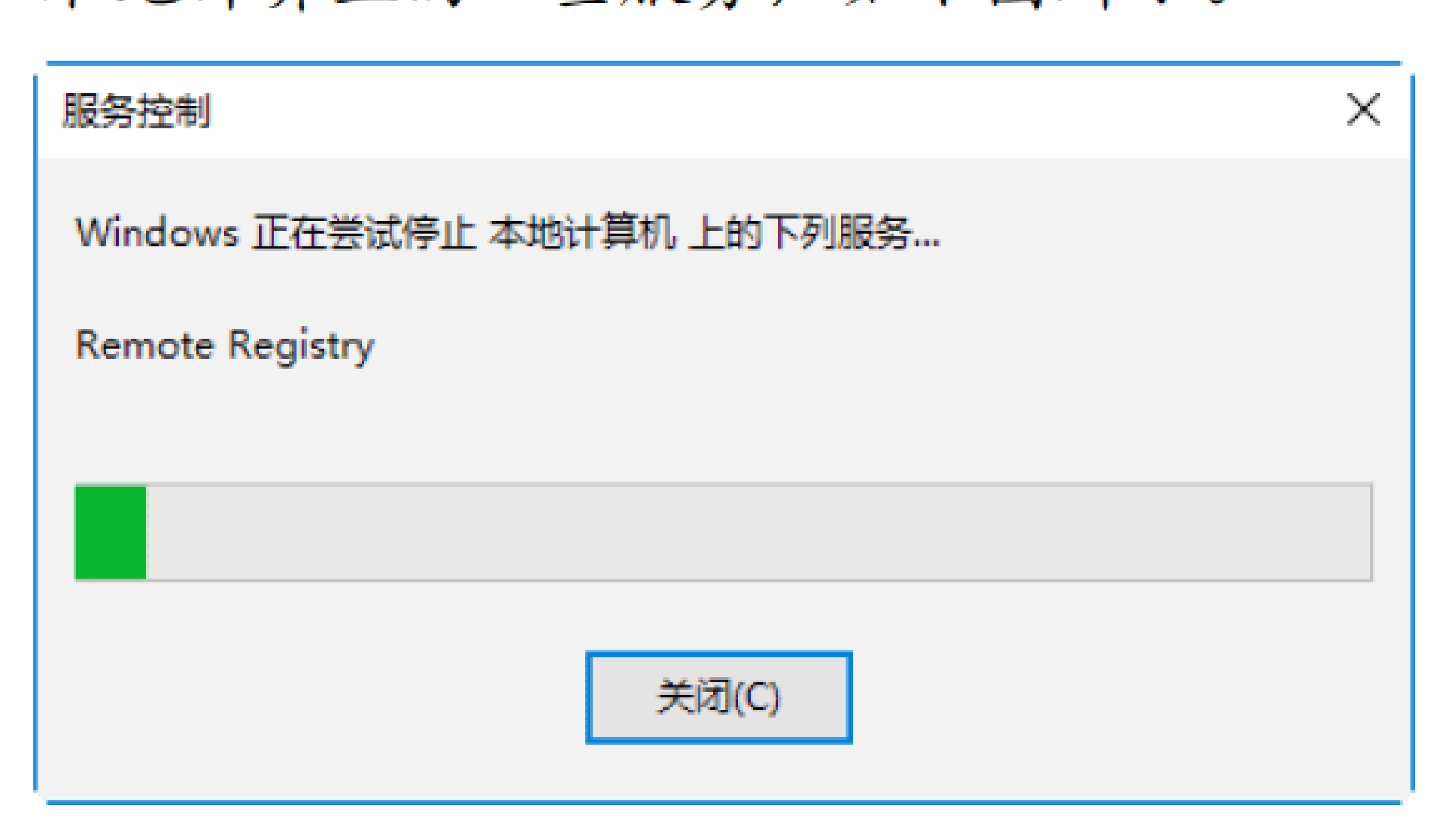
Step 02 双击“服务”选项，打开“服务”窗口，在其中可看到本地计算机中的所有服务，如下图所示。



Step 03 在“服务”列表中选中Remote Registry选项并右击，在弹出的快捷菜单中选择“属性”选项，打开“Remote Registry的属性”对话框，如下图所示。



Step 04 单击“停止”按钮，即可打开“服务控制”提示框，提示Windows正在尝试停止本地计算上的一些服务，如下图所示。



Step 05 在服务停止完毕之后，即可返回到“Remote Registry的属性”对话框，此时即可看到“服务状态”已变为“已停止”，单击“确定”按钮，即可完成“允许远程注册表操作”服务的关闭操作，如下图所示。

6.6　实战演练

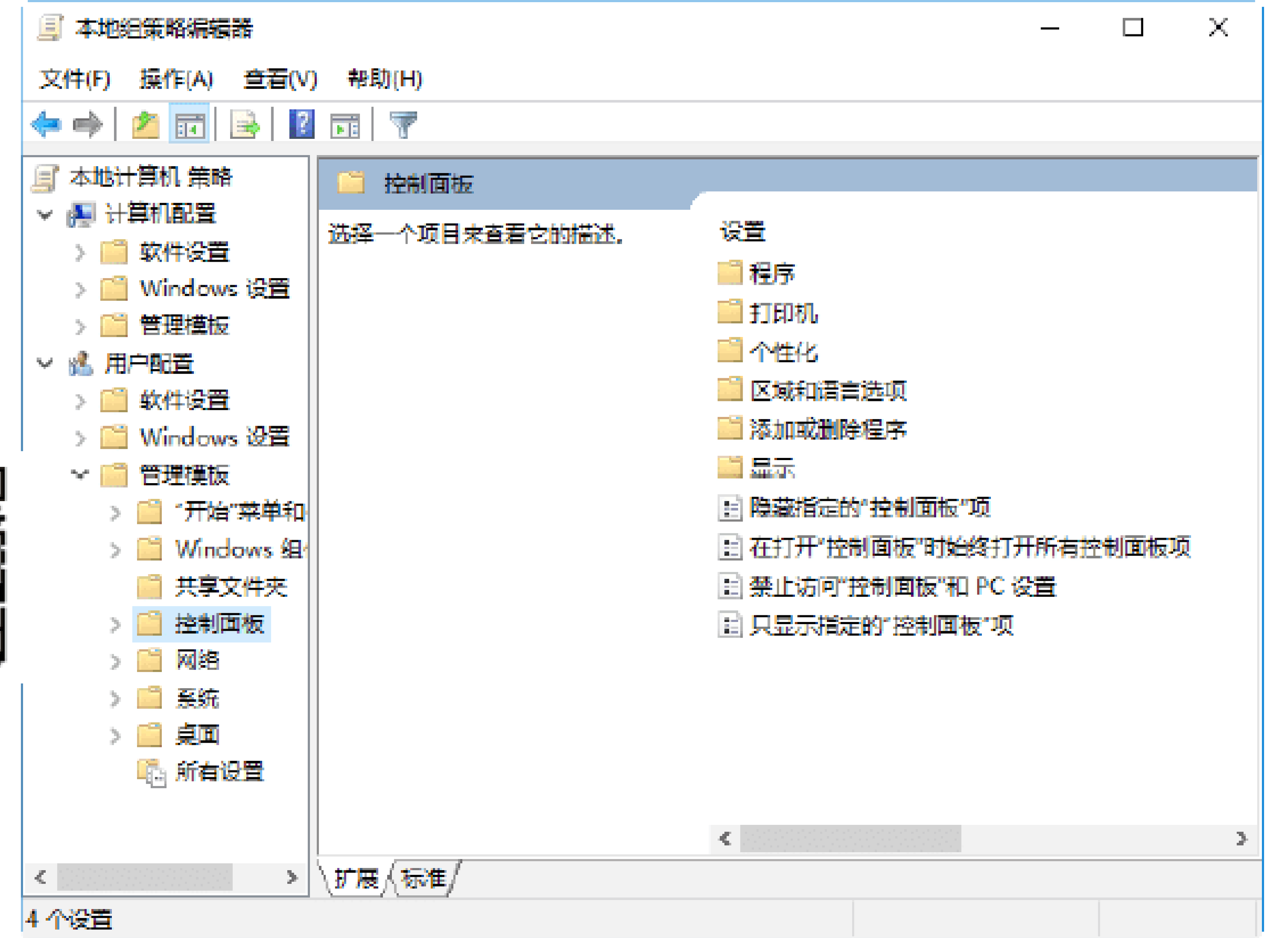
实战演练1——禁止访问计算机控制面板



黑客可以通过控制面板进行多项系统的操作，用户若不希望他们访问自己的控制面板，可以在“本地组策略编辑器”窗

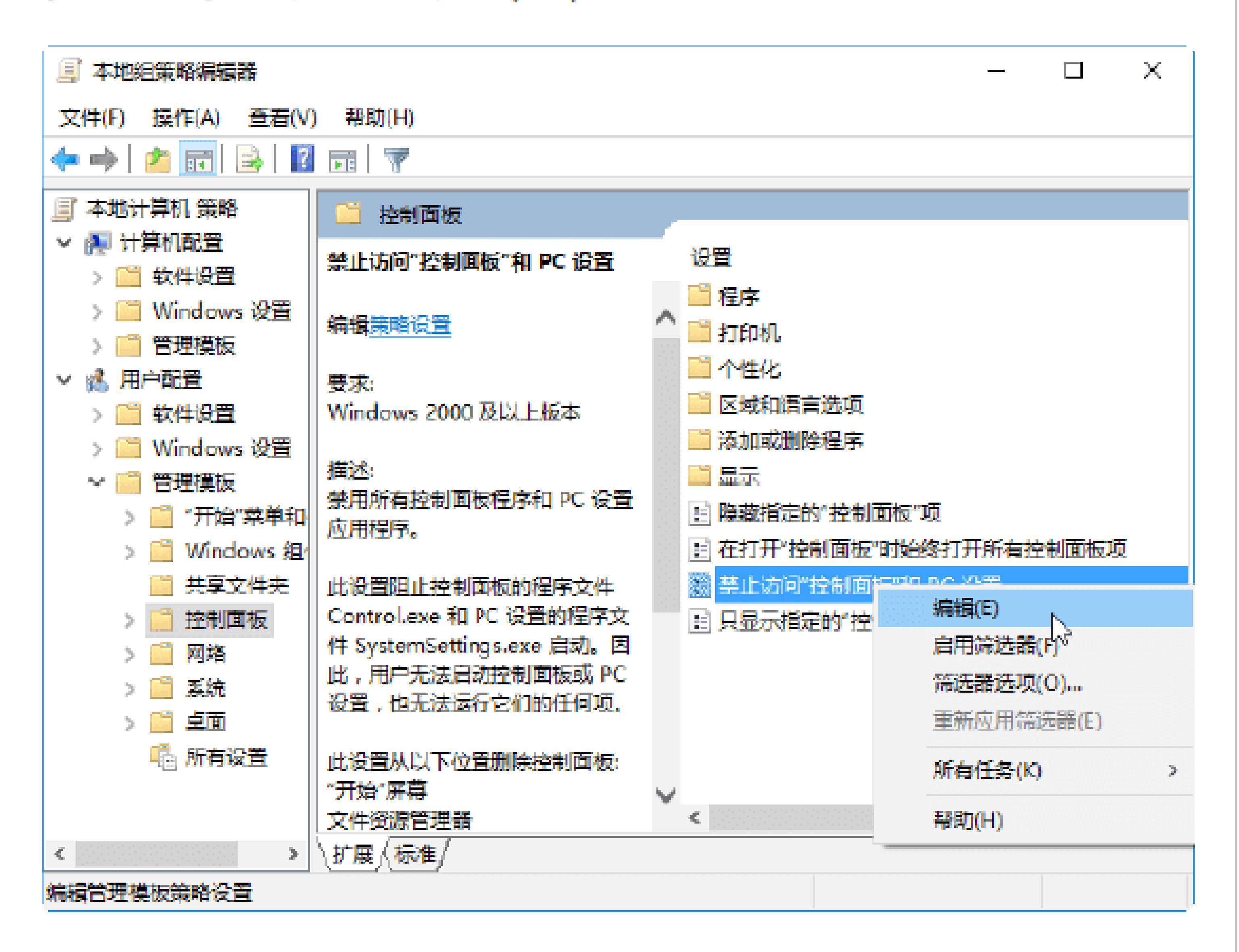
口中启用“禁止访问控制面板”功能。具体的操作步骤如下。

Step 01 打开“本地组策略编辑器”窗口，在其中依次展开“用户配置”→“管理模板”→“控制面板”选项，即可进入“控制面板”设置界面，如下图所示。

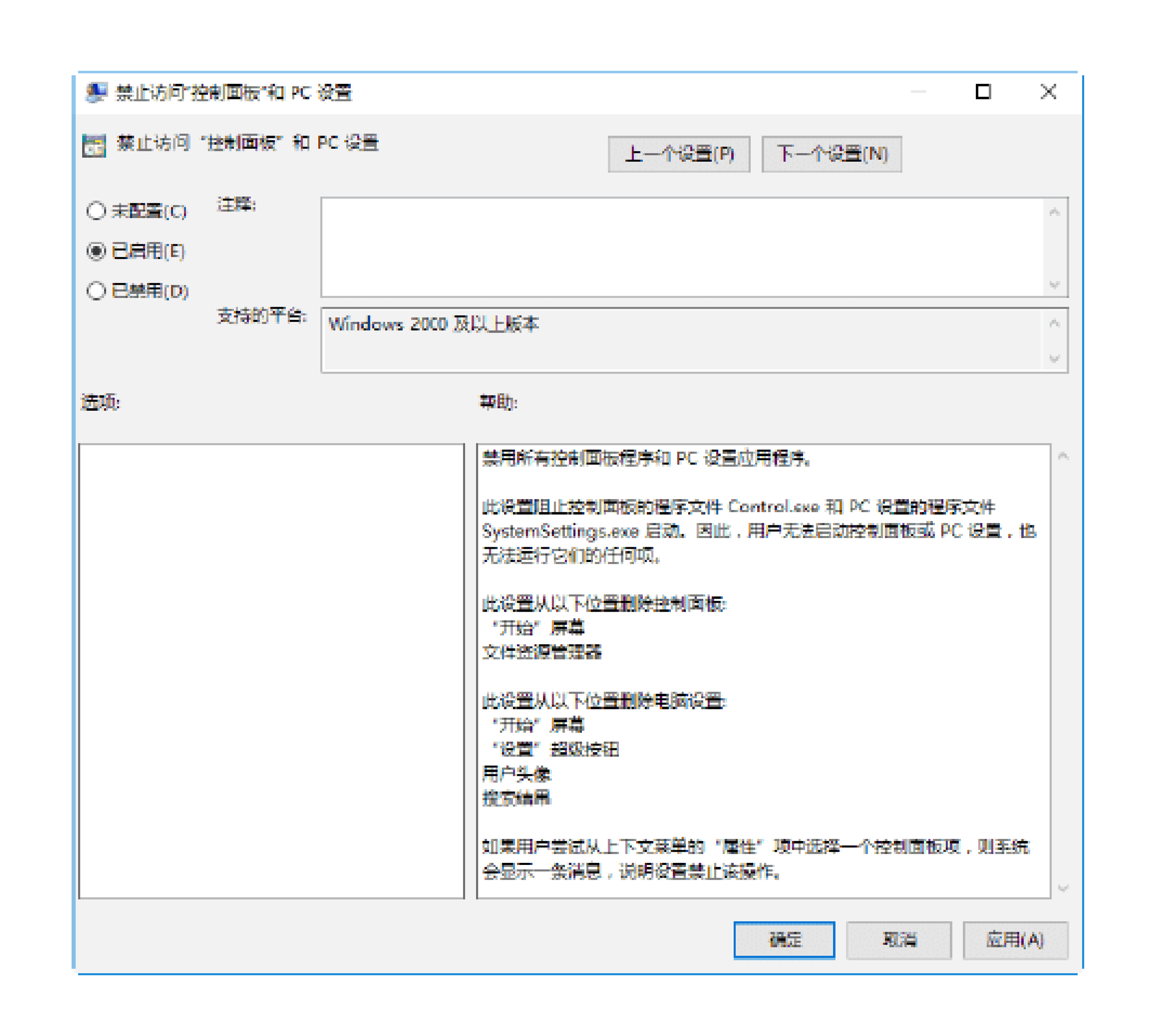




Step 02 右击“禁止访问控制面板和PC设置”选项，在快捷菜单中选择“编辑”选项，或双击“禁止访问‘控制面板’和PC设置”选项，如下图所示。



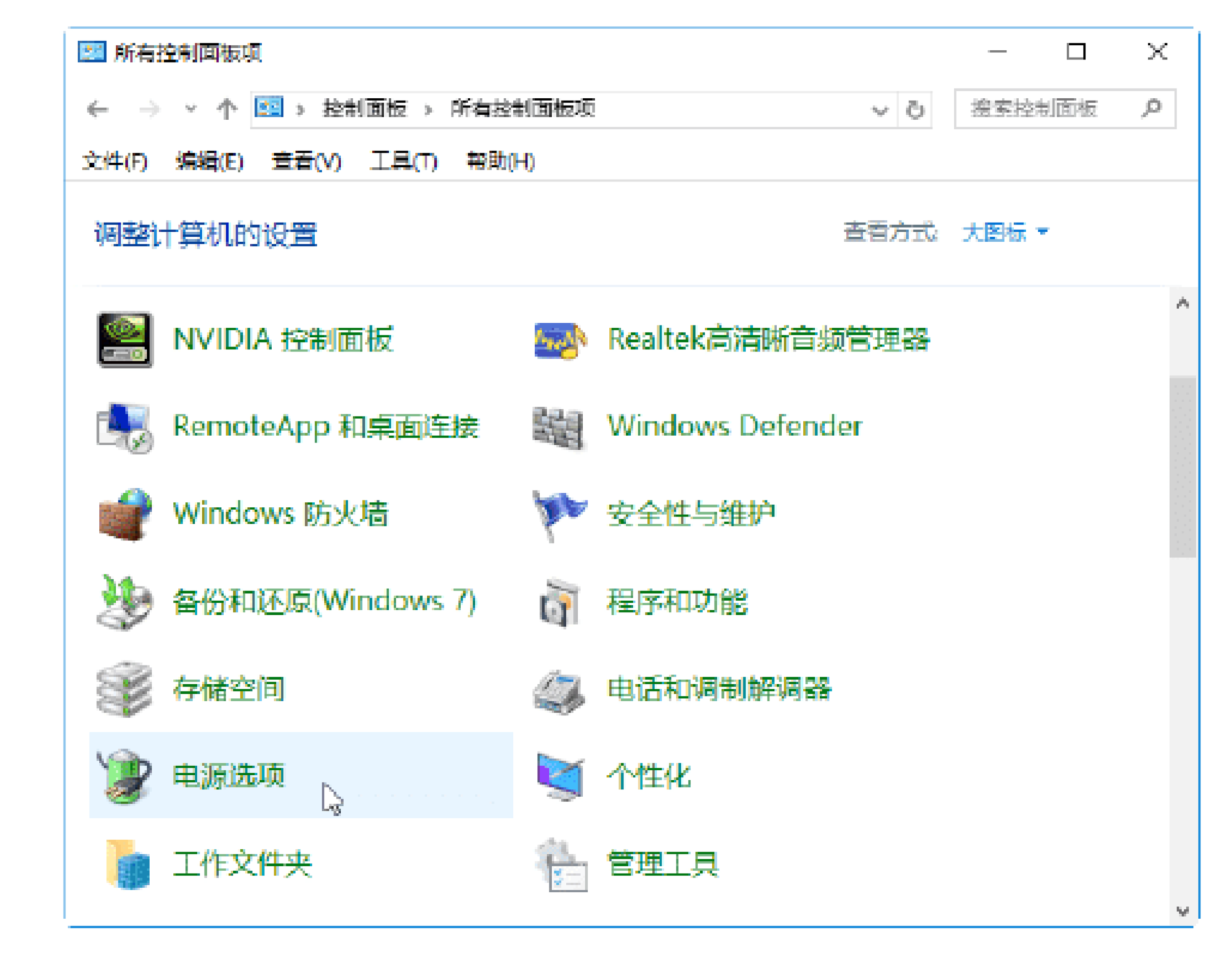
Step 03 打开“禁止访问‘控制面板’和 PC 设置”对话框，在其中选中“已启用”单选按钮，单击“确定”按钮，即可完成禁止控制面板程序文件的启动，使得其他用户无法启动控制面板，如下图所示。此时，还会将“开始”菜单中的“控制面板”选项、Windows资源管理器中的“控制面板”文件夹同时删除，彻底禁止访问控制面板。



实战演练2——启用和关闭快速启动功能

使用系统中的“启用快速启动”功能，可以加快系统的开机启动速度。启用和关闭快速启动功能的具体操作步骤如下。

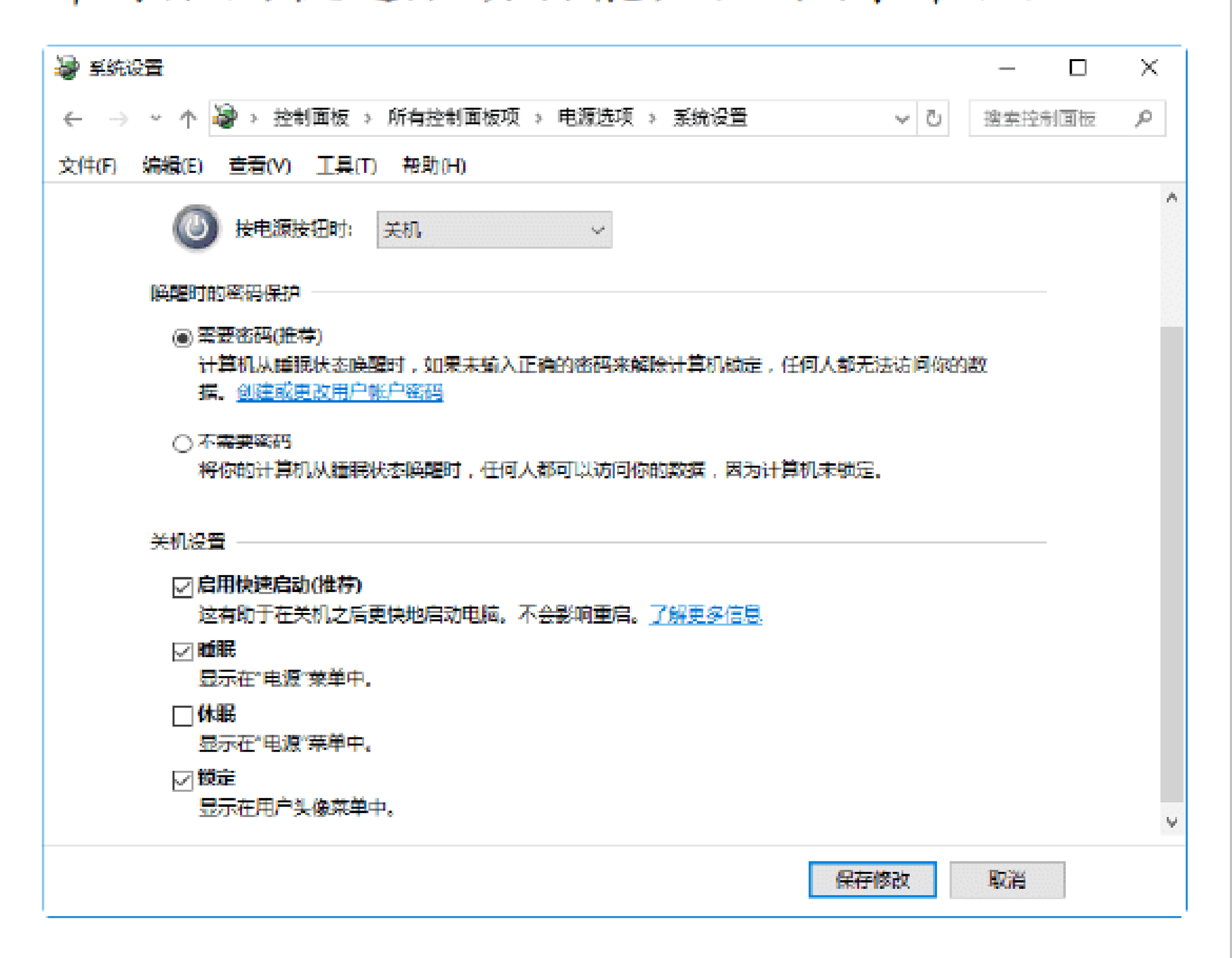
Step 01 单击“开始”按钮，在弹出的快捷菜单中选择“控制面板”选项，打开“所有控制面板项”窗口，如下图所示。



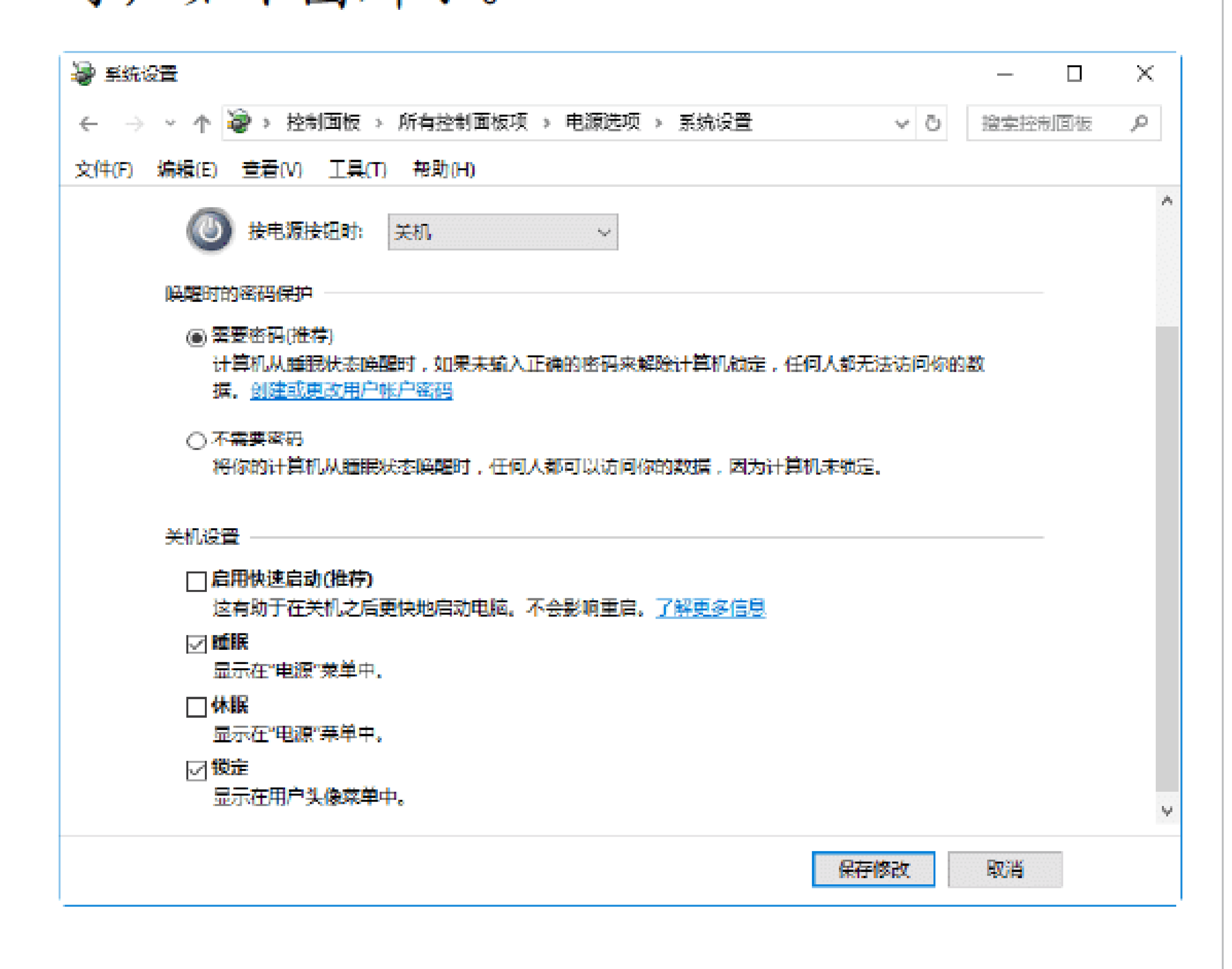
Step 02 单击“电源选项”图标，打开“电源选项”设置界面，如下图所示。



Step 03 单击“选择电源按钮的功能”超链接，打开“系统设置”窗口，在“关机设置”区域中勾选“启用快速启动（推荐）”复选框，单击“保存修改”按钮，即可启用快速启动功能，如下图所示。



Step 04 如果想要关闭快速启动功能，则可以取消对“启用快速启动（推荐）”复选框的勾选，然后单击“保存修改”按钮即可，如下图所示。

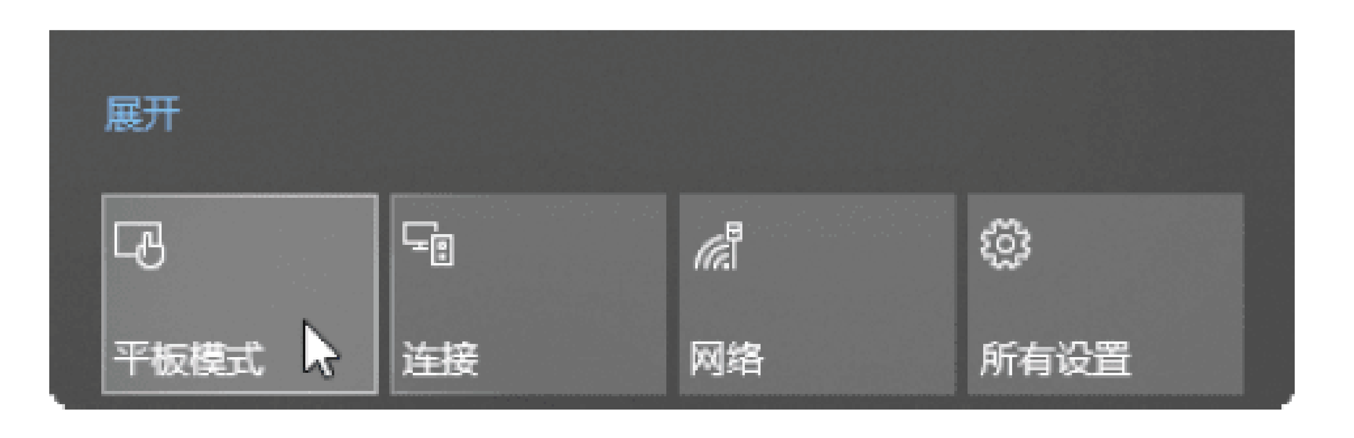


6.7　小试身手

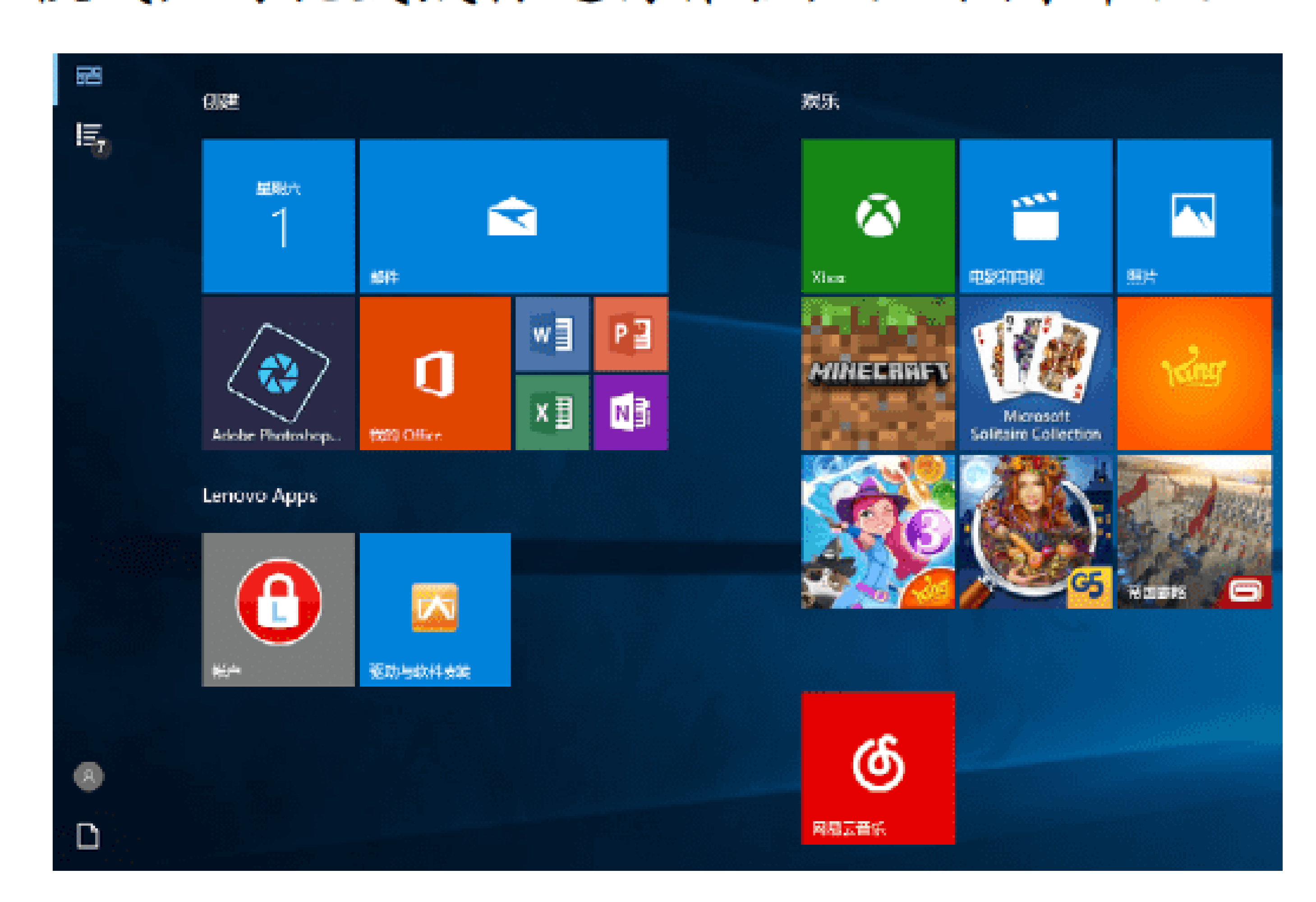
练习1：开启系统的平板模式

Windows 10新增了一种使用模式——平板模式，它可以使计算机像平板计算机那样使用。开启平板模式的操作如下。

Step 01 单击桌面右下角通知区域中的“通知”图标，在弹出的窗口中单击“平板模式”图标，如下图所示。



Step 02 返回桌面，即可看到系统桌面变为平板模式，可拖曳鼠标进行体验，如下图所示。



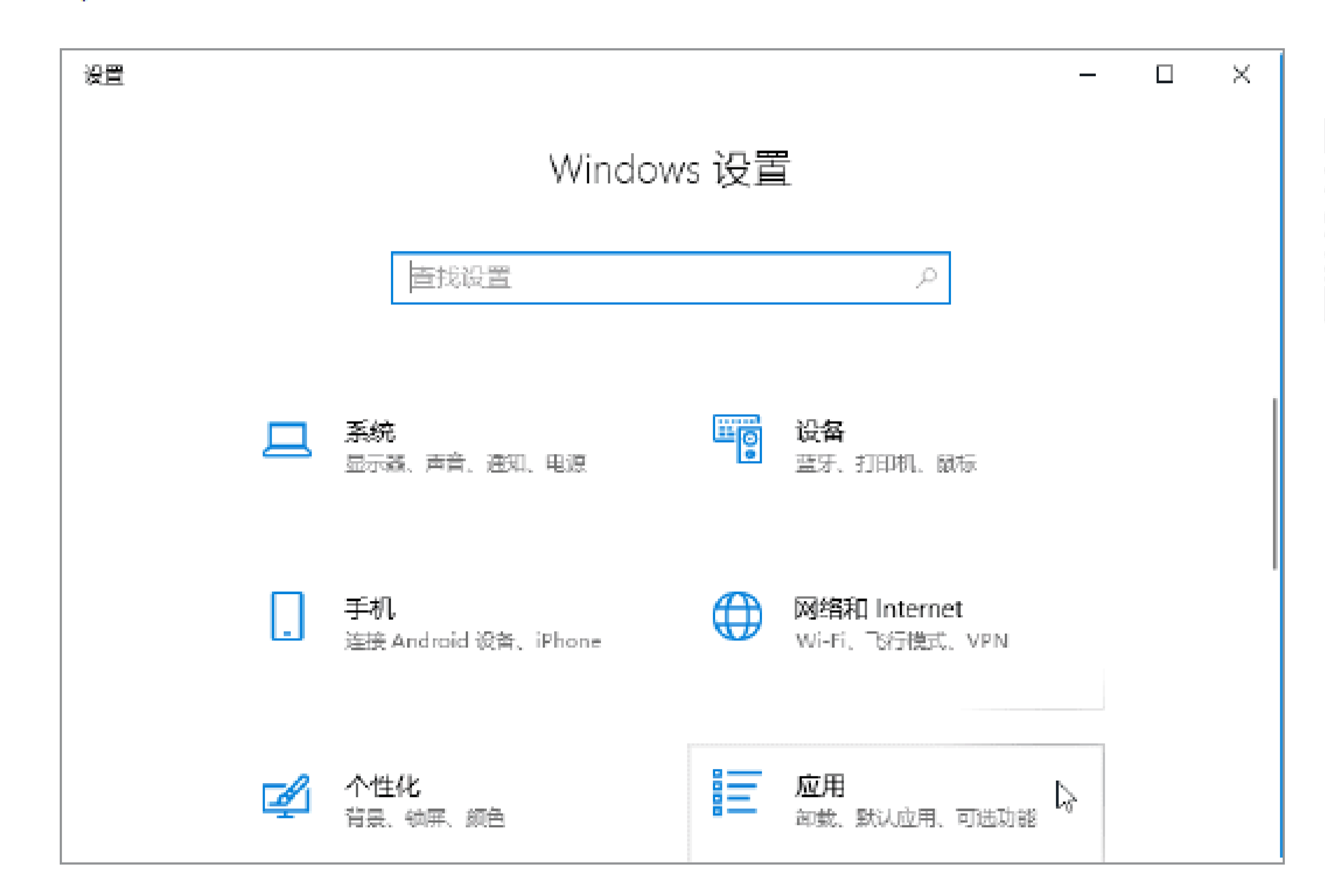
Step 03 如果计算机支持触屏操作，则体验效果更佳。如要退出平板模式，则再次单击“平板模式”图标即可，如下图所示。



练习2：设置默认打开应用程序

一个应用可能有多种打开方式，有时希望用默认的应用来打开特定的文件，就可以设置默认打开程序。在Windows 10操作系统中设置默认打开应用程序的具体操作步骤如下。

Step 01 按WIN+I组合键，打开“设置”面板，并单击“应用”图标选项，如下图所示。





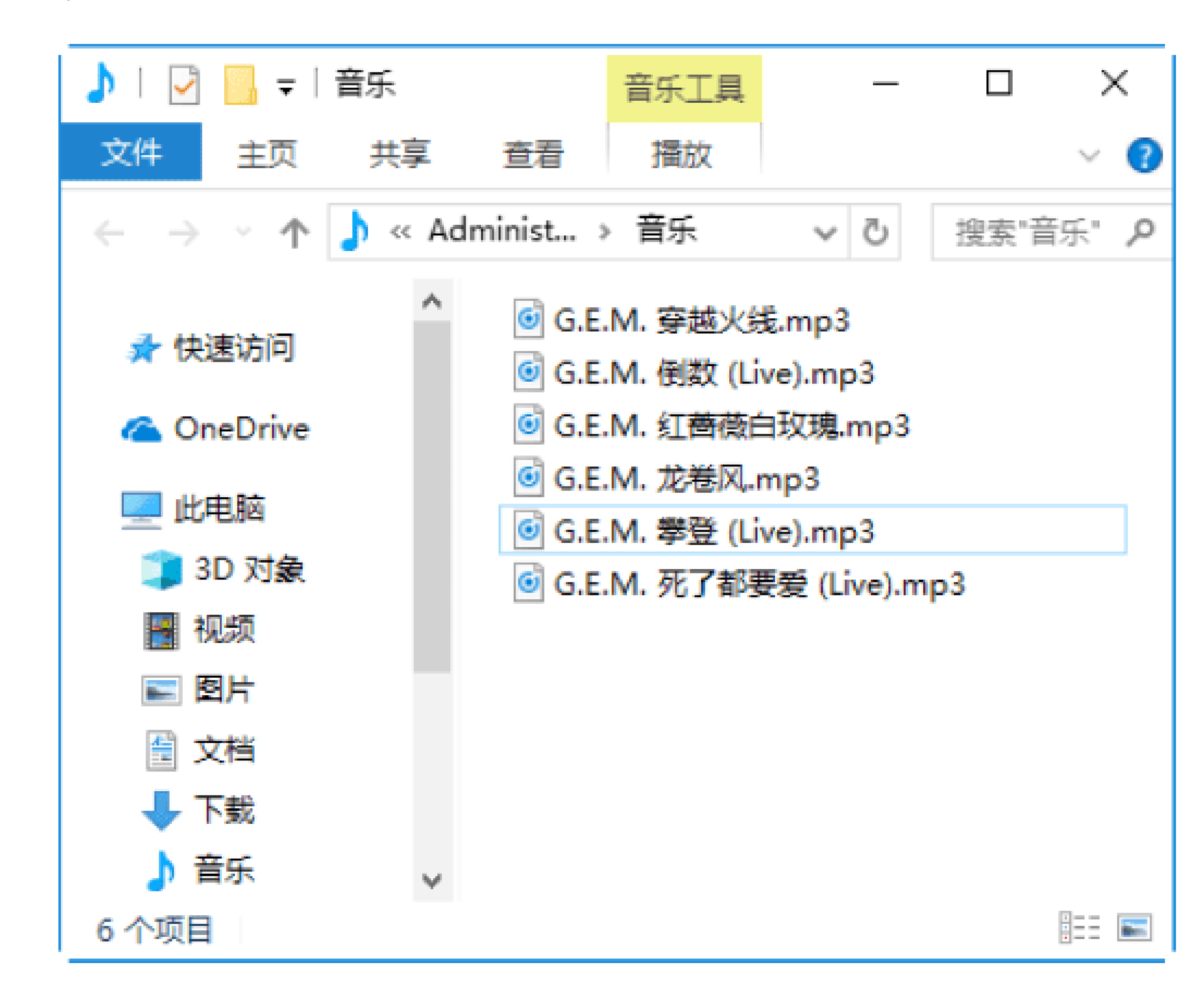
Step 02 单击“应用”界面左侧的“默认应用”选项，即可看到电子邮件、地图、音乐播放器等默认打开的应用，如下图所示。



Step 03 在要改变默认打开应用图标上单击，弹出“选择应用”列表，选择要使用的应用程序，即可进行更改，如下图所示，这里将音乐播放器的打开程序设置为“Groove音乐”。



Step 04 在对应的文件中，如歌曲类型的文件，则变为Groove音乐的图标，如下图所示。



第7章　网络账号及密码的安全防护

随着网络用户的飞速增长，各种各样的网络账号也越来越多，账号密码被盗的现象也屡见不鲜。本章介绍网络账号及密码的防护策略，主要内容包括QQ账号及密码的安全防护、微信账号及密码的安全防护以及网银账号及密码的安全防护等。

7.1　QQ账号及密码的安全防护

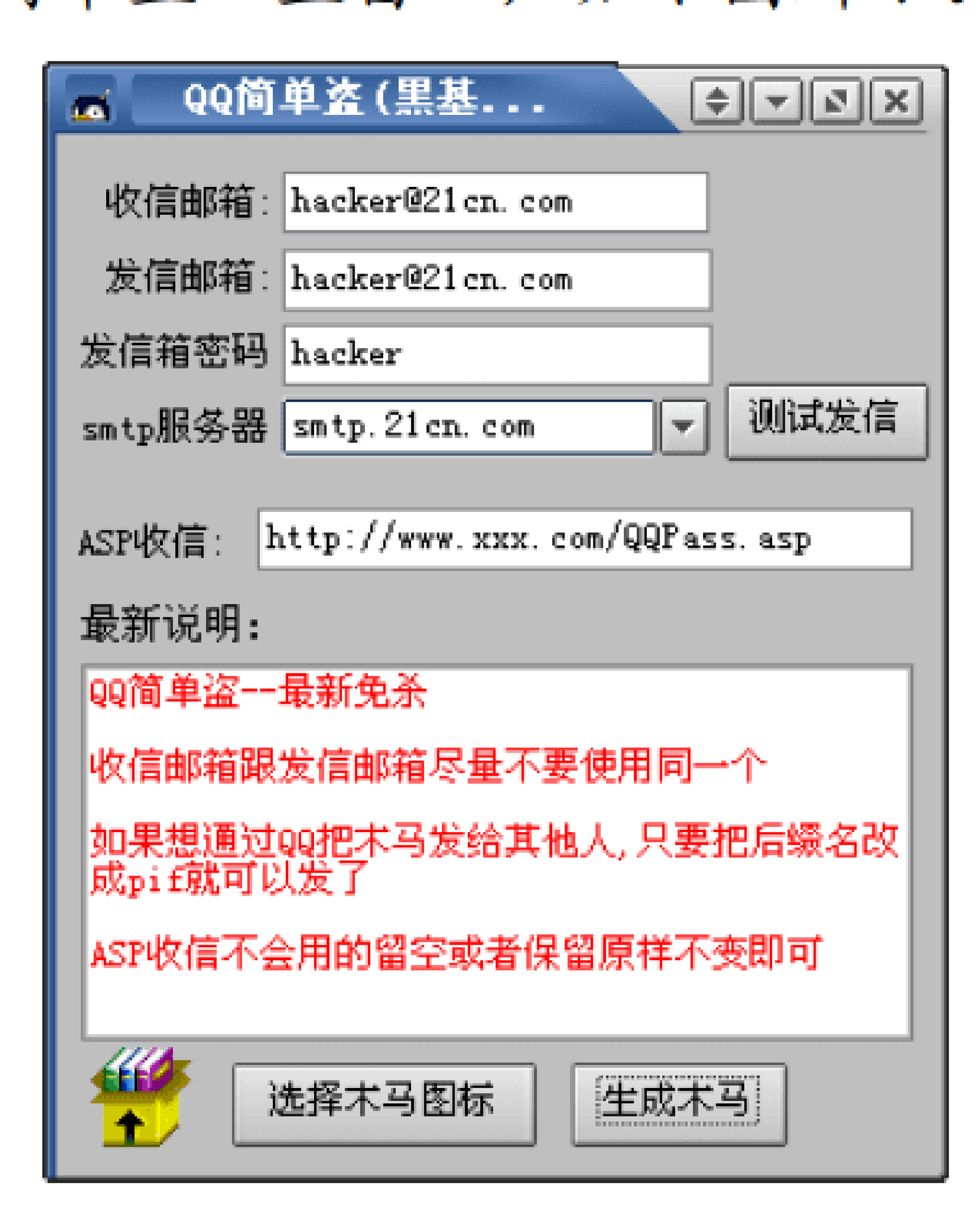
QQ聊天打破了广大网民地域的限制，可以和任何地方的朋友进行交流，方便了工作和生活。但是随着QQ的普及，一些盗取QQ账号与密码的黑客也活跃起来。

实战1：盗取QQ账号与密码

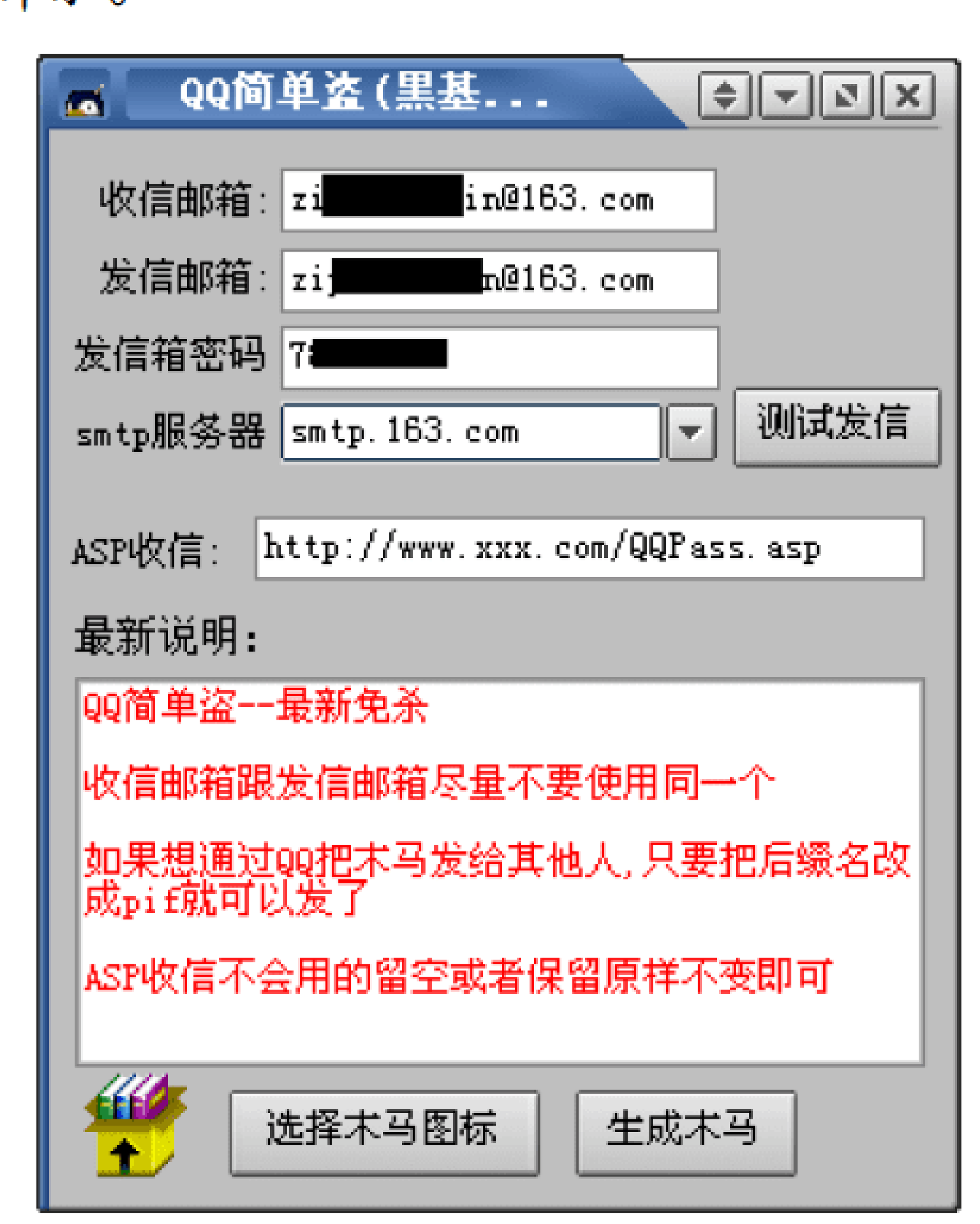
“QQ简单盗”是一款经典的盗号软件，采用插入技术，本身不产生进程，因此难以被发现。它会自动生成一个木马，只要黑客将生成的木马发送给目标用户，并诱骗其运行该木马文件，就达到了入侵的目的。

使用“QQ简单盗”盗取密码的具体操作步骤如下。

Step 01 下载并解压“QQ简单盗”文件夹，双击“QQ简单盗.exe”应用程序，打开“QQ简单盗”主窗口，如下图所示。



Step 02 在“收信邮箱”“发信邮箱”和“发信箱密码”等文本框中分别输入邮箱地址和密码等信息；在“smtp服务器”下拉列表框中选择一种邮箱的smtp服务器，如下图所示。



Step 03 设置完毕后，单击“测试发信”按钮，打开“请察看您的邮箱是否收到测试信件”提示框，如下图所示。



Step 04 单击OK按钮，然后在IE地址栏中输入邮箱的网址，进入“邮箱登录”页面，在其中输入设置的收信邮箱账户和密码，即可进入该邮箱首页，如下图所示。



Step 05 双击接收到的“测试发信”邮件，进入该邮件的相应页面，当收到“QQ简单盗发信测试”这样的信息，则表明“QQ简单盗”发消息功能正常，如下图所示。

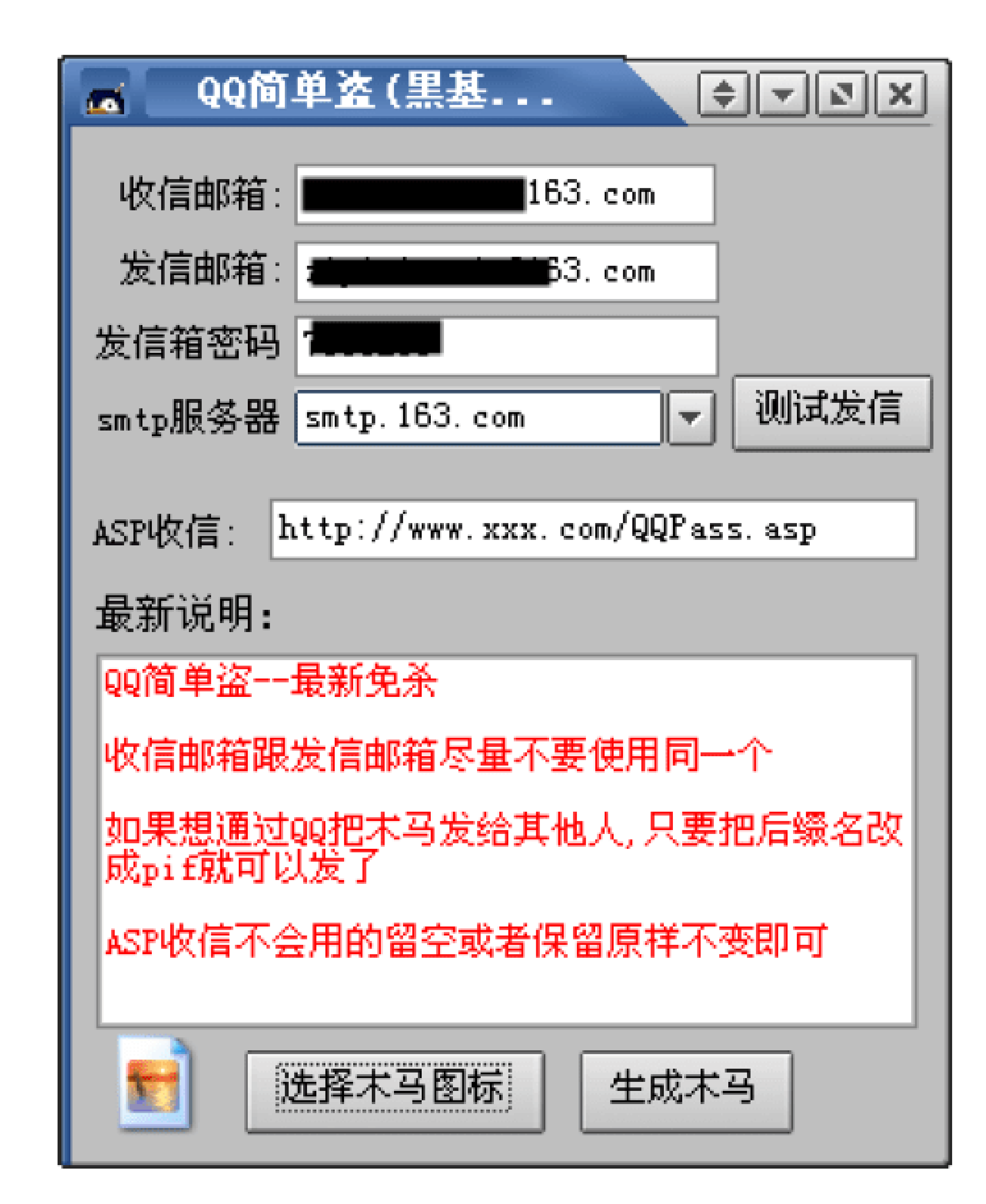


提示：一旦“QQ简单盗”截获到QQ的账号和密码，会立即将内容发送到指定的邮箱。

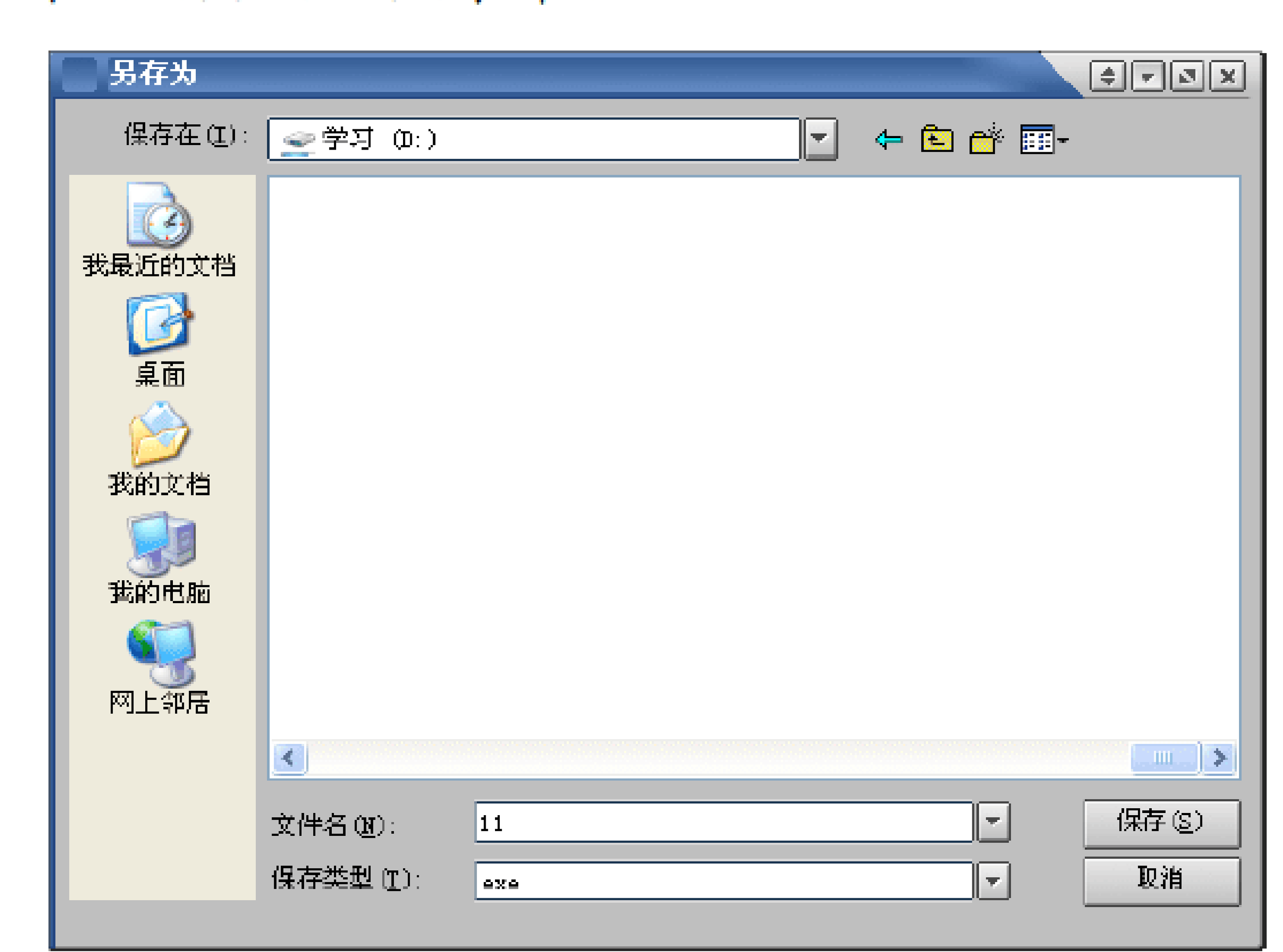
Step 06 在“QQ简单盗”主窗口中单击“选择木马图标”按钮，打开“打开”对话框，根据需要选择一个常见的、不易被人怀疑的文件做图标，如下图所示。



Step 07 单击“打开”按钮，返回“QQ简单盗”主窗口，在窗口的左下方即可看到木马图标已经换成了普通图片，如下图所示。



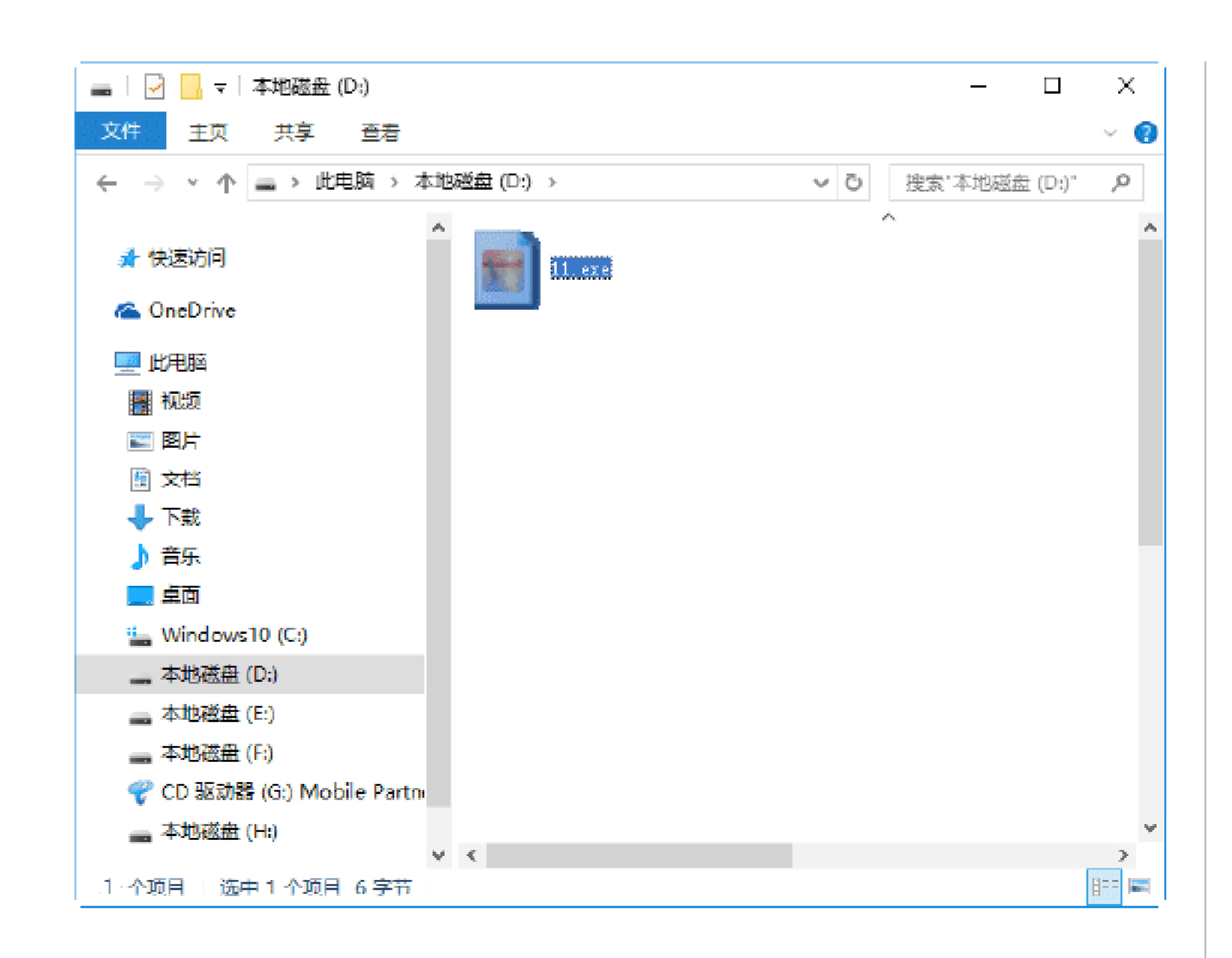
Step 08 单击“生成木马”按钮，打开“另存为”对话框，在其中设置存放木马的路径和名称，如下图所示。



Step 09 单击“保存”按钮，打开“提示”提示框，在其中显示生成的木马文件的存放路径和名称，如下图所示。



Step 10 单击“确定”按钮，即可成功生成木马。打开存放木马所在的文件夹，即可看到做好的木马程序，如下图所示。此时盗号者会将它发送出去，哄骗QQ用户去运行它，即可完成植入木马操作。

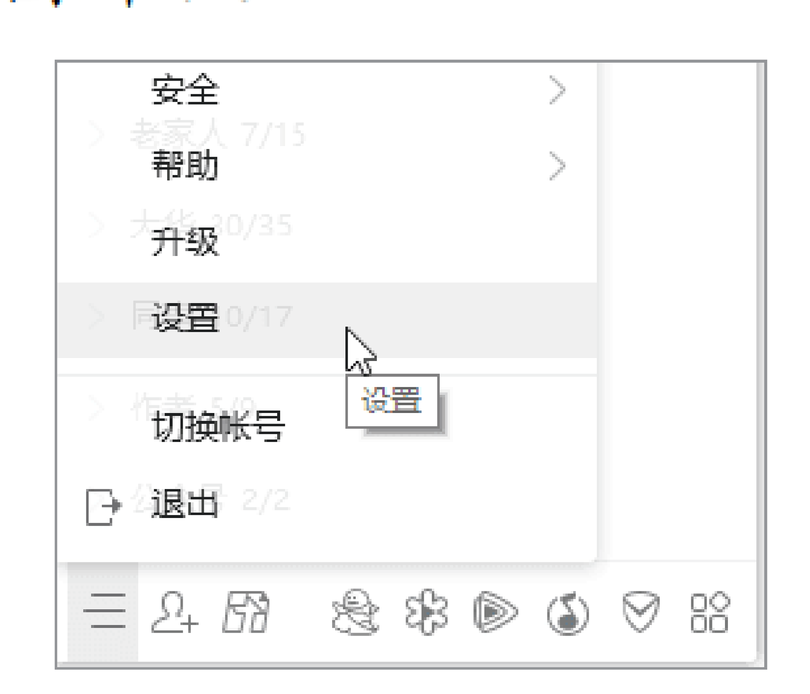


实战2：提升QQ账号的安全设置

QQ提供保护用户隐私和安全的功能。通过QQ的安全设置，可以很好地保护用户的个人信息和账号的安全。

具体操作步骤如下。

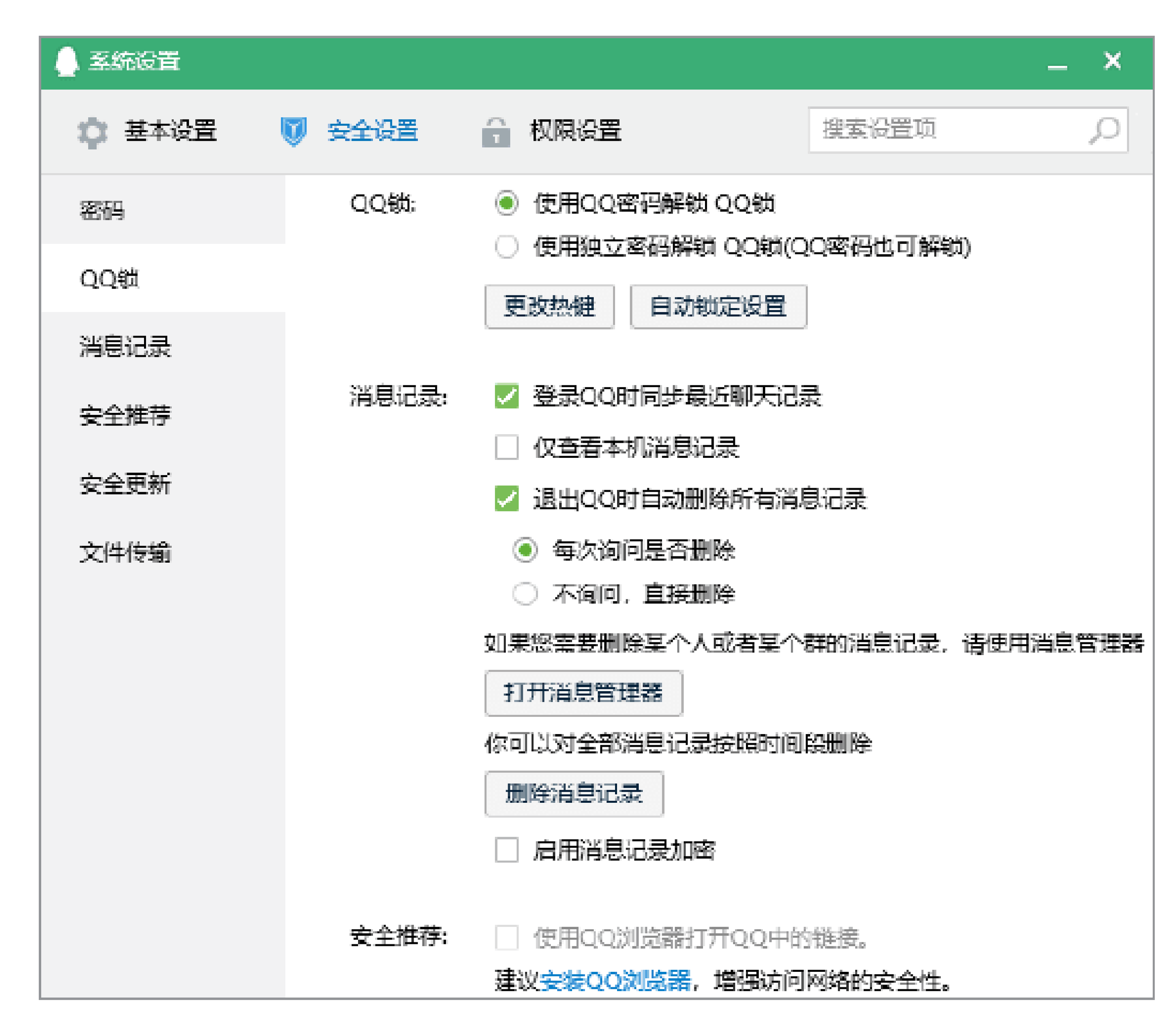
Step 01 打开QQ主界面，单击“主菜单”按钮，在弹出的列表中选择“设置”菜单命令，如下图所示。



Step 02 弹出“系统设置”对话框，选择“安全设置”选项，用户可以修改密码、设置QQ锁和文件传输的安全级别等，如下图所示。



Step 03 选择“QQ锁”选项，用户可以设置QQ加锁功能，如下图所示。



Step 04 选择“消息记录”选项，勾选“退出QQ时自动删除所有消息记录”复选框，并勾选“启用消息记录加密”复选框，然后输入相关口令，还可以设置加密口令提示，如下图所示。





Step 05 选择“安全推荐”选项，QQ建议安装QQ浏览器，从而增强访问网络的安全性，如下图所示。



Step 06 选择“安全更新”选项，用户可以设置安全更新的安装方式，一般选中“有

安全更新时自动为我安装，无须提醒（推荐）”单选按钮，如下图所示。



Step 07 选择“安全防护”选项，在其中可以设置浏览器的防钓鱼功能，如下图所示。



Step 08 选择“文件传输”选项，在其中可以设置文件传输的安全级别，一般采用推荐设置即可，如下图所示。



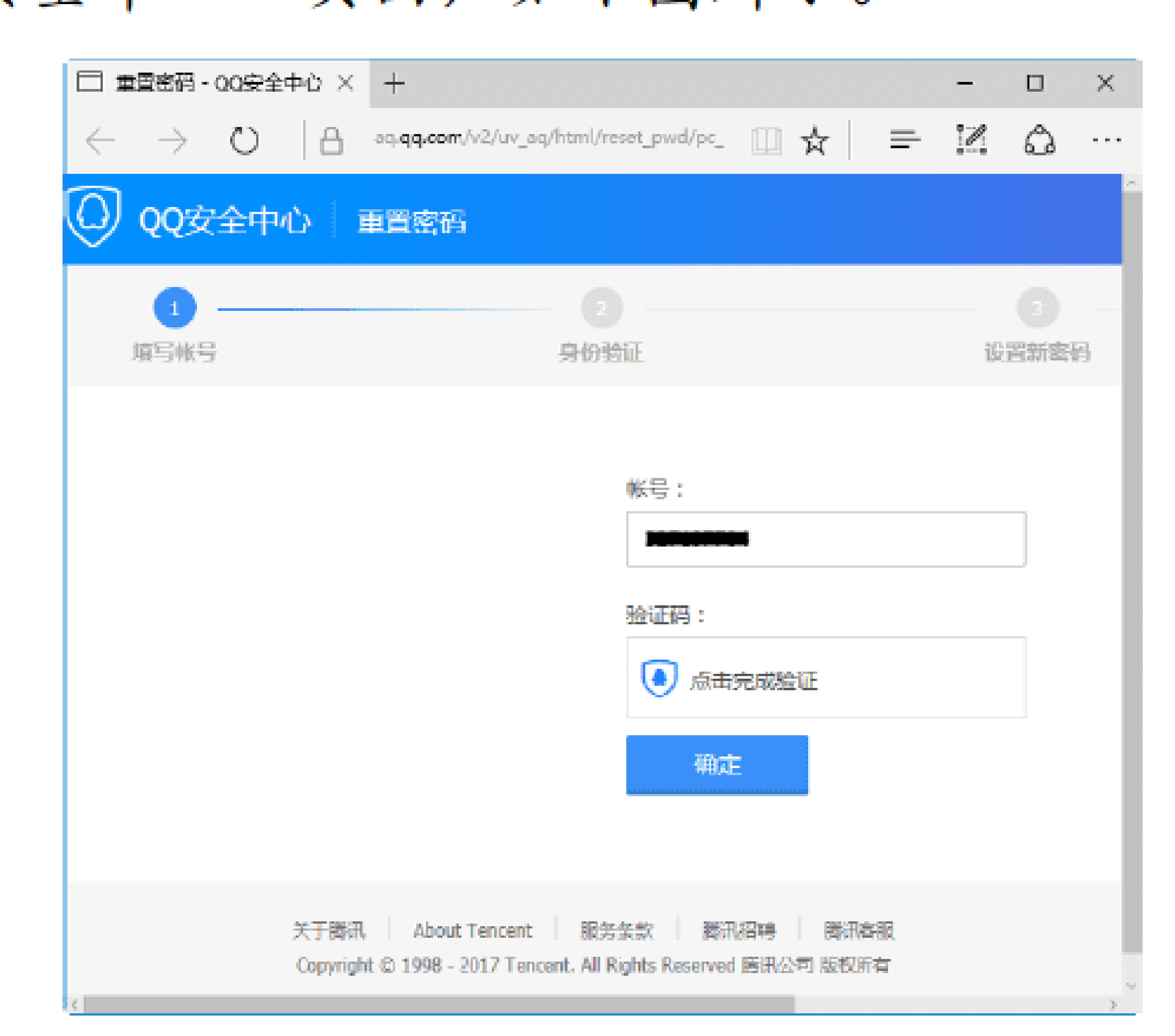
实战3：找回被盗的QQ账号密码

通过QQ申诉可以找回密码，但是在找回密码的过程中，需要用户自己的QQ好友辅助配合才行。通过QQ申诉找回密码的具体操作步骤如下。

Step 01 双击桌面上的QQ登录快捷图标，打开QQ登录窗口，如下图所示。



Step 02 单击“找回密码”链接，进入“QQ安全中心”页面，如下图所示。



Step 03 单击“点击完成验证”链接，打开验证页面，在其中根据提示完成安全验证，如下图所示。



Step 04 单击“验证”按钮，完成安全验证，提示用户验证通过，如下图所示。

帐号：
[redacted]
验证码：
验证通过
确定

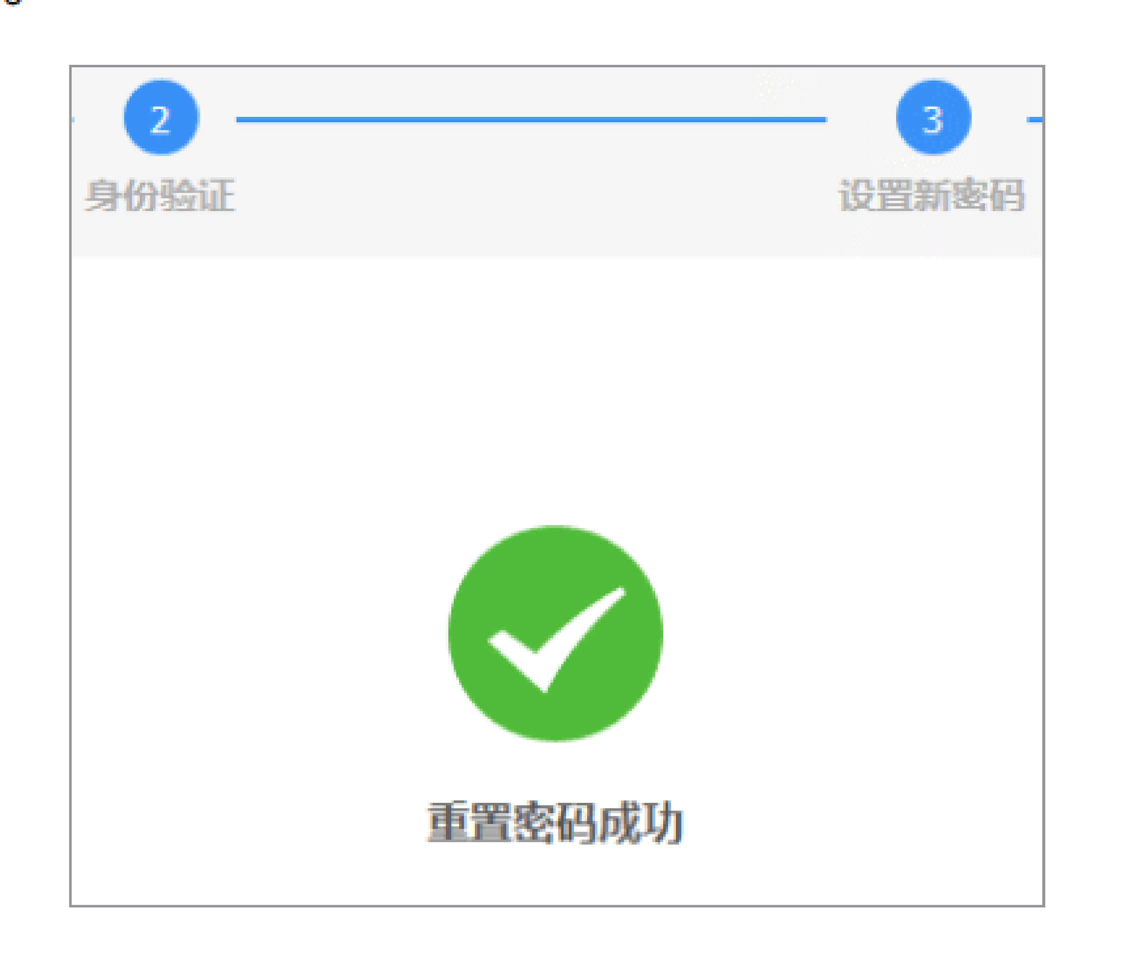
Step 05 单击“确定”按钮，进入“身份验证”页面，在其中单击“免费获取验证码”按钮，这时QQ安全中心会给密保手机发送一个验证码，在下面的文本框中输入收到的验证码，如下图所示。

2 身份验证　3 设置新密码
经过智能小安的检测，本次操作需要您通过以下方式确认身份
请用密保手机181******81获取短信验证码　已换号？
免费获取验证码
已发送，今天免费短信已用完　没收到短信？
[redacted]
确定
短信用不了？更换其他验证方式

Step 06 单击“确定”按钮，进入“设置新密码”页面，在其中输入设置的新密码，如下图所示。



Step 07 单击“确定”按钮，重置密码成功，这样就找回了被盗的QQ账号密码，如下图所示。



7.2　微信账号及密码的安全防护

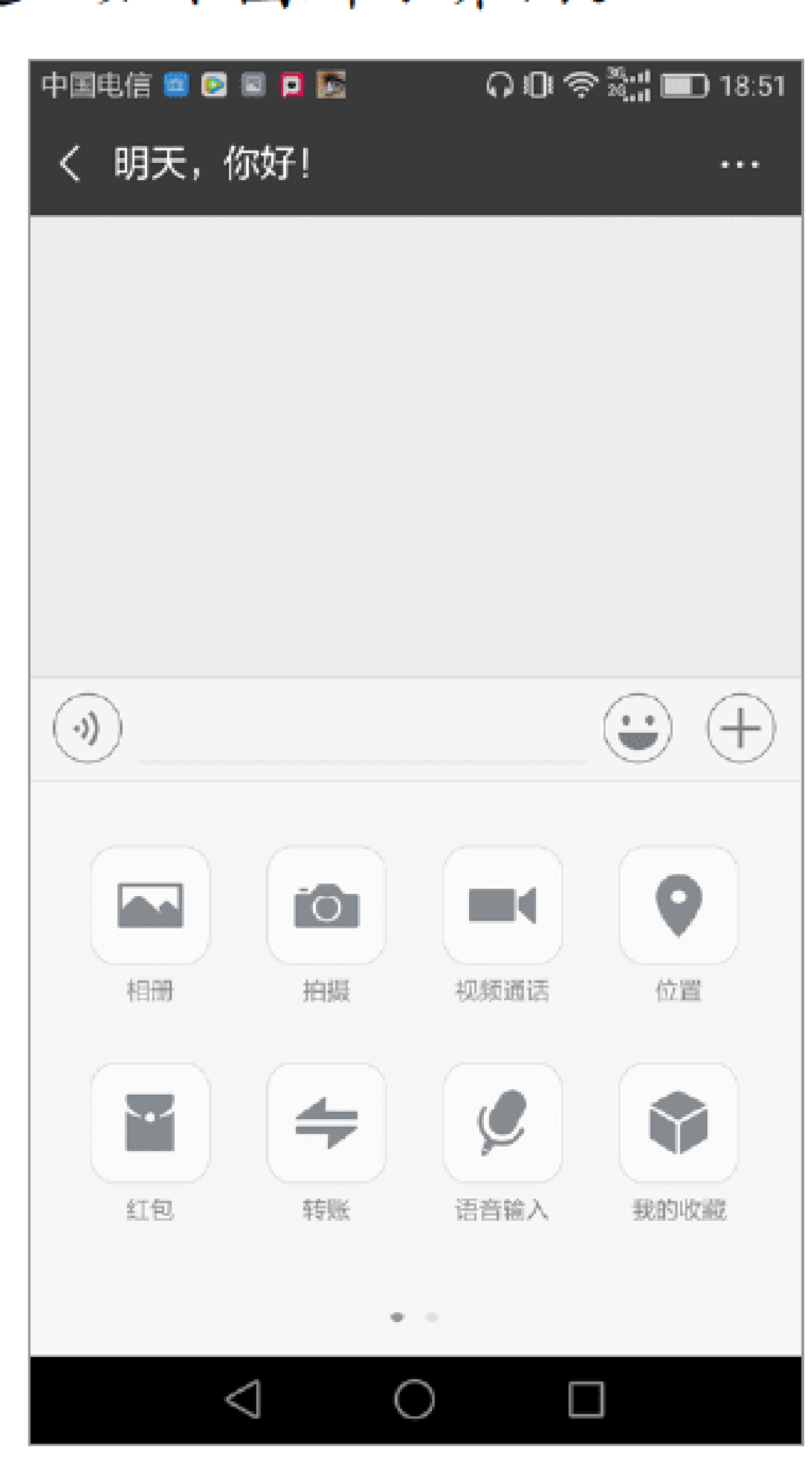
微信是一个为智能终端提供即时通信服务的免费应用程序，支持语音短信、视频、图片和文字等多种沟通方式，用户还可以群聊，并支持支付功能。为此，保护微信账号及密码的安全就显得非常重要。

实战4：使用微信手机钱包转账

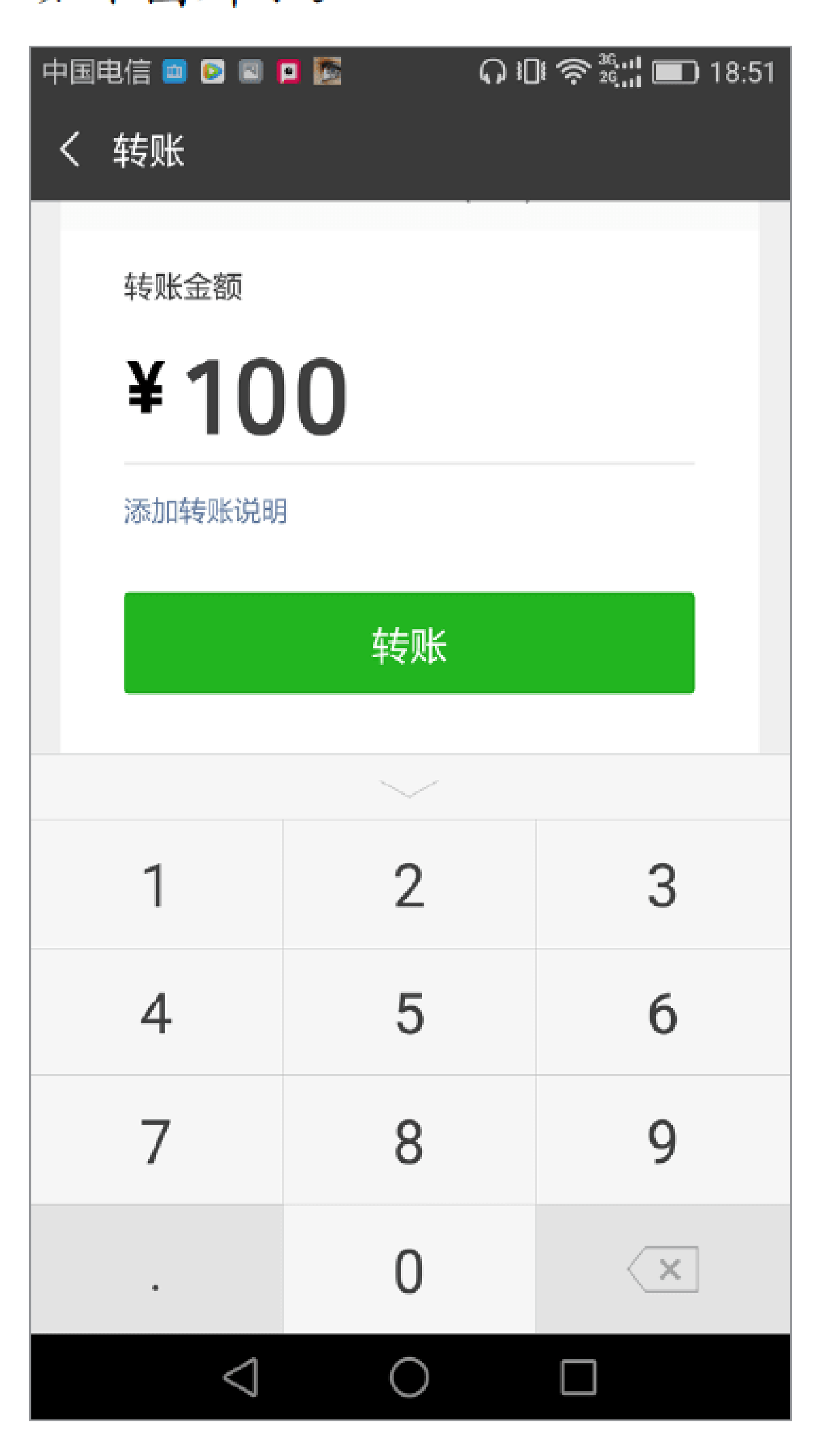


使用手机钱包转账是目前比较流行的支付方式，下面介绍使用手机钱包转账的方法与步骤。

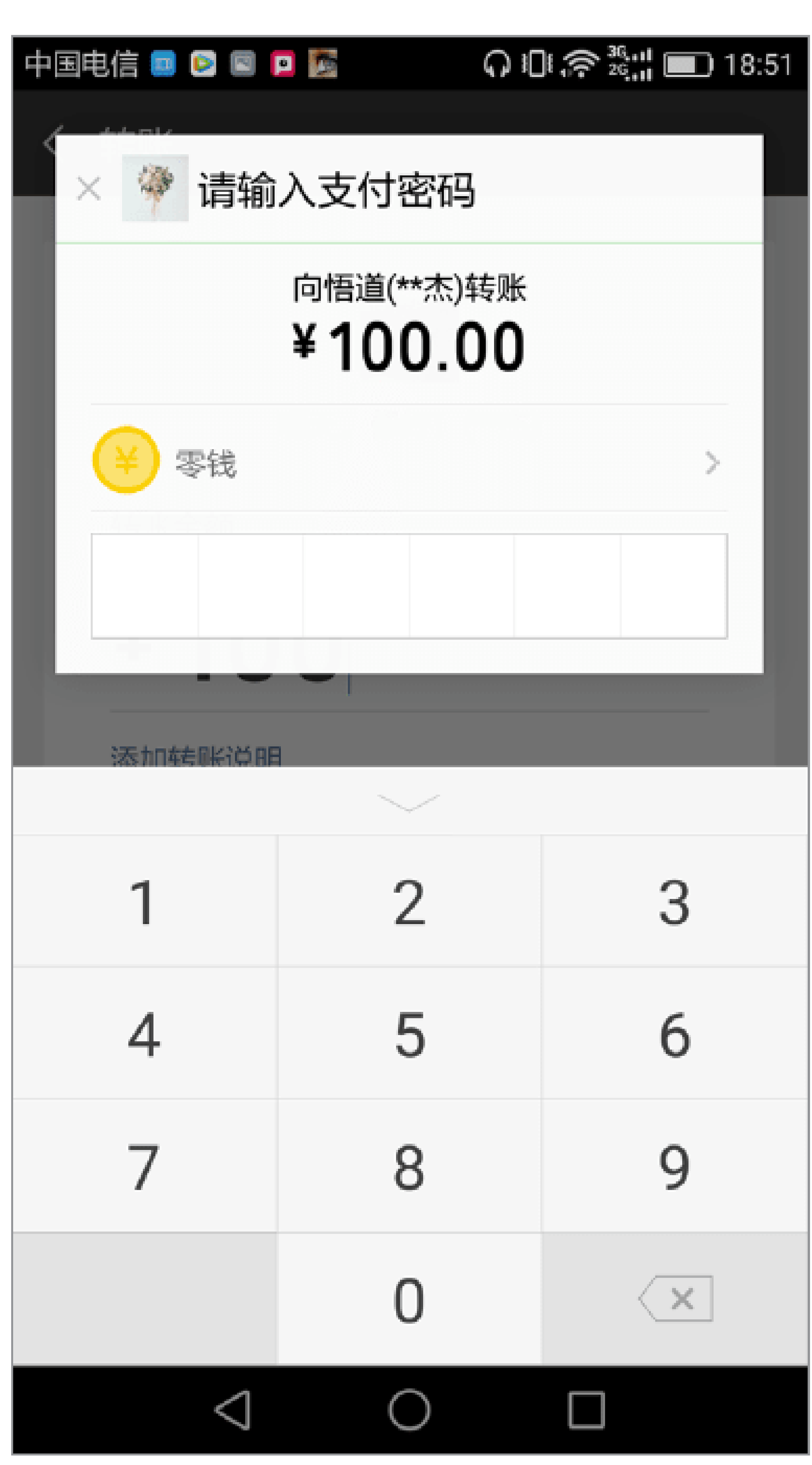
Step 01 登录微信，点按需要给予转账的用户，进入微信聊天界面，点按右侧的“⊕”图标，进入如下图所示界面。



Step 02 点按“转账”图标，进入“转账”界面，在其中输入转账金额，如这里输入100，如下图所示。



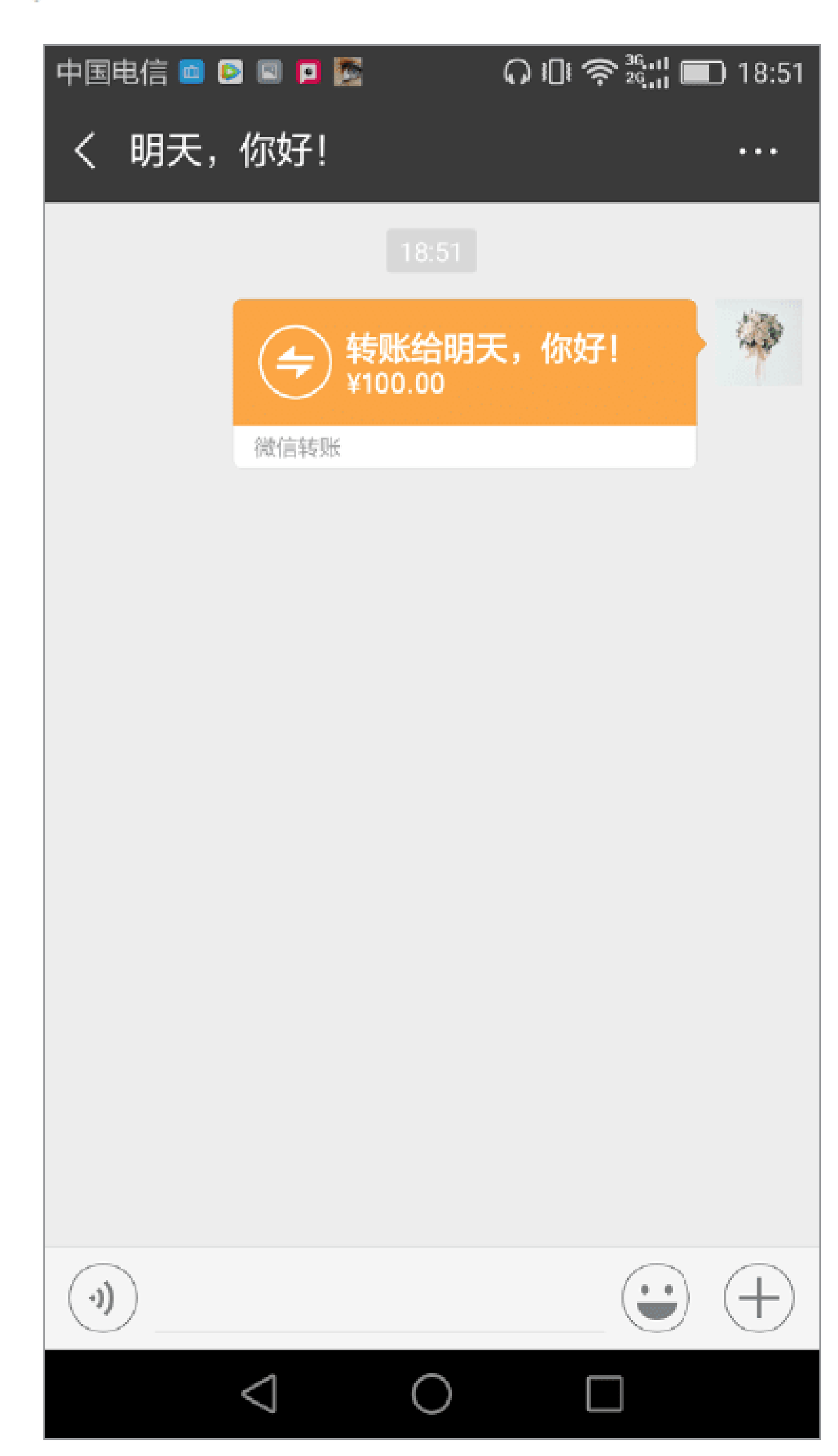
Step 03 点按“转账”按钮，进入“请输入支付密码”界面，在其中需要输入支付密码，如下图所示。



Step 04 输入密码正确后，会弹出“支付成功”界面，如下图所示。



Step 05 点按“完成”按钮，即可将红包发送给对方，并显示发送的金额，如下图所示。



Step 06 当对方收钱后，会返回一个对方已收钱的信息提示，如下图所示。



实战5：微信支付的安全设置

微信支付已经是当前流行的支付方式了，因此，对微信手机钱包的安全设置非常重要。安全设置的操作步骤如下。

Step 01 在手机微信中进入"我的钱包"页面，如下图所示。



Step 02 点按右上角的"▦"图标，进入"支付中心"页面，如下图所示。

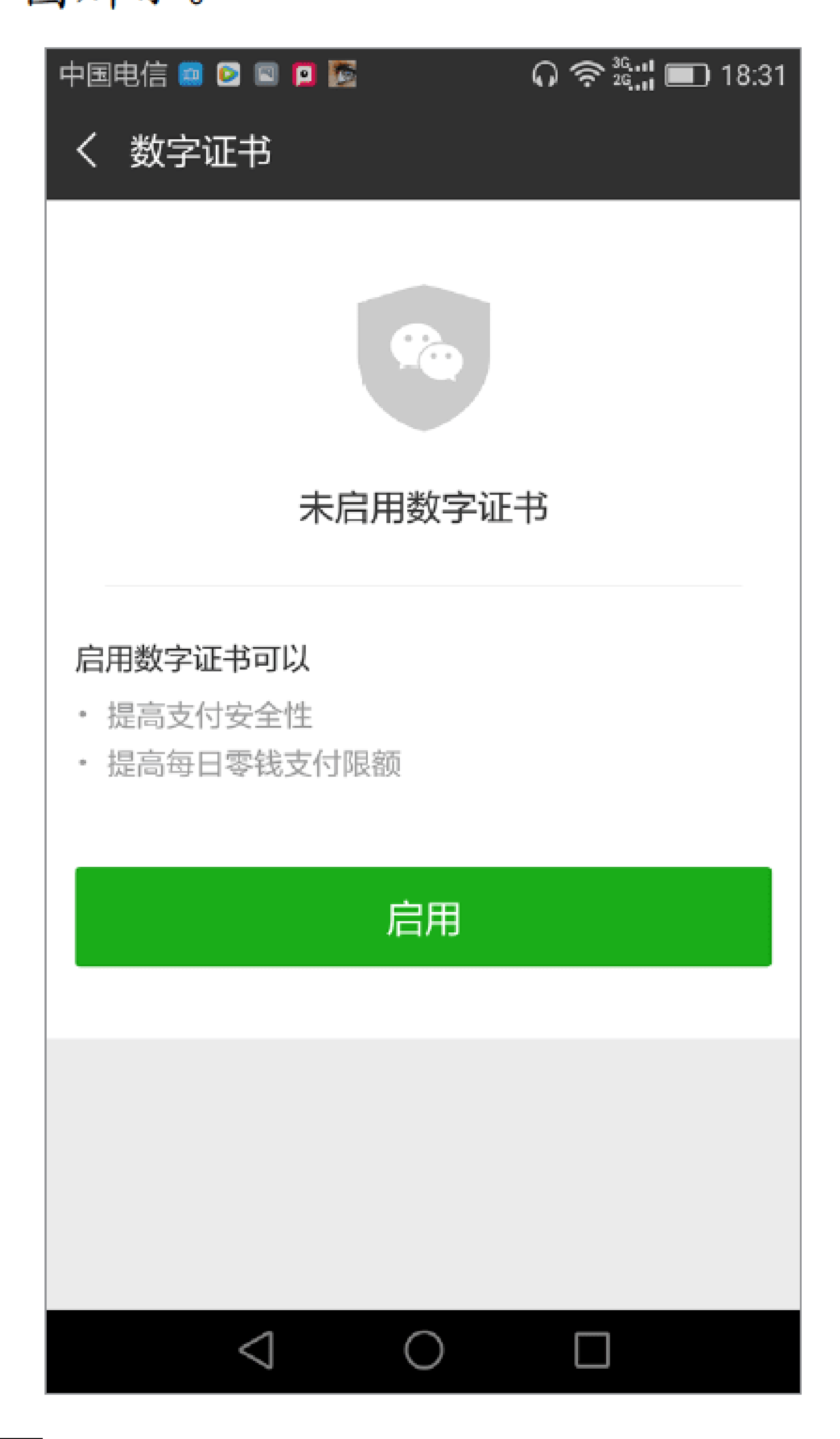




Step 03 点按"支付安全"选项，进入"支付安全"界面，在其中可以选择更多的安全设置，如下图所示。



Step 04 点按“数字证书”选项，进入“数字证书”界面，提示用户未启用数字证书，如下图所示。



Step 05 点按“启用”按钮，进入“启用数字证书”界面，在其中输入身份证号，如下图所示。



Step 06 点按“验证”按钮，即可开始验证身份信息，验证完成后，会给出相应的提示信息，如下图所示。



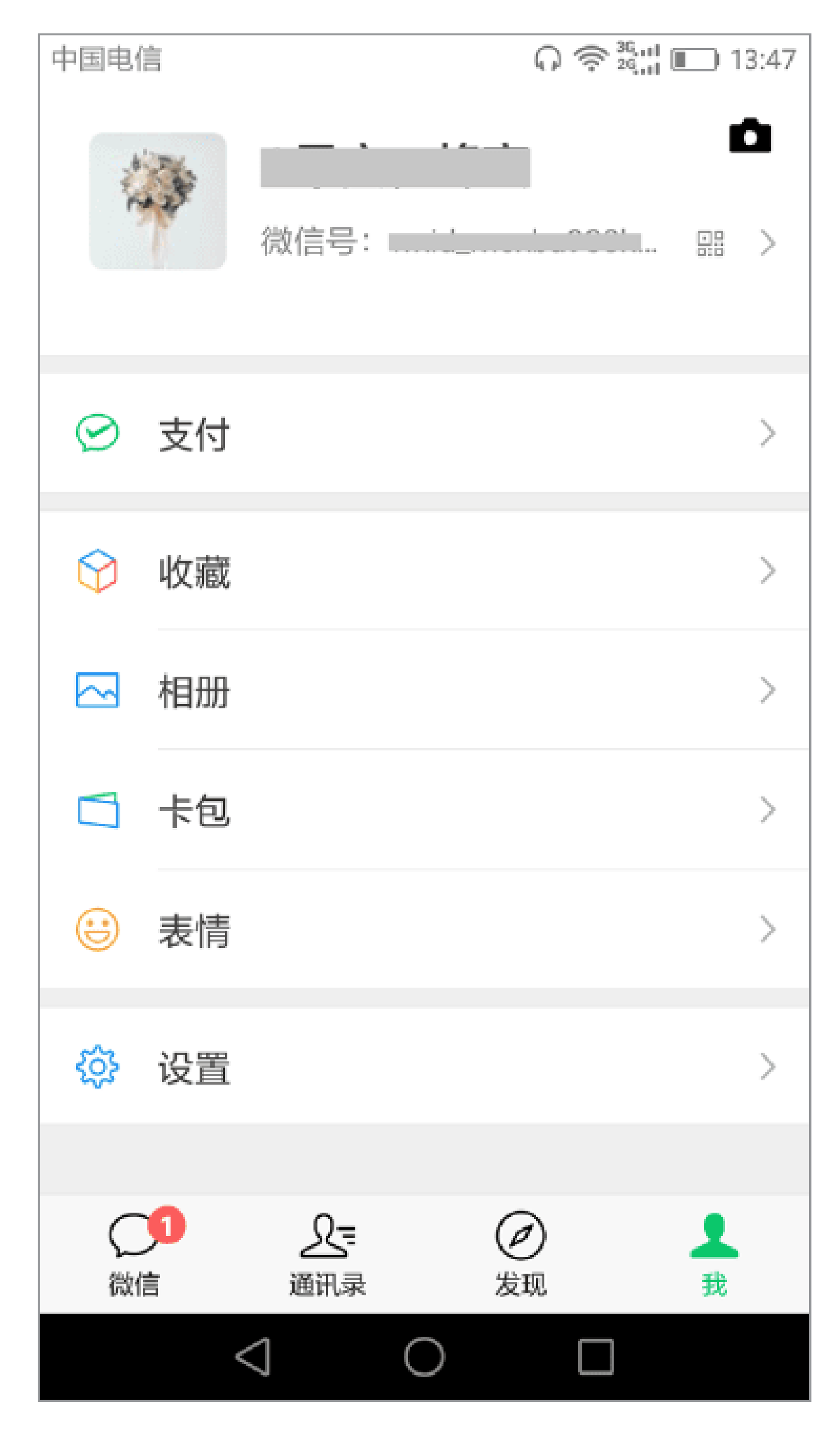
Step 07 返回到“支付安全”界面，在其中可以看到数字证书已经启用，使用同样的方法还可以启动“钱包锁”功能，如下图所示。



实战6：冻结微信账号以保护账号安全

当发现自己的微信账号被盗或手机丢失时，用户可以通过冻结微信号来保护账号安全。具体操作步骤如下。

Step 01 在微信的工作界面中，点按“我”图标，进入“我”设置界面，如下图所示。



Step 02 点按“设置”选项，进入“设置”界面，如下图所示。

中国电信 13:48
设置
帐号与安全
新消息提醒
勿扰模式
聊天
隐私
通用
关于微信
帮助与反馈
插件

Step 03 点按“账号与安全”选项，进入“账号与安全”设置界面，如下图所示。

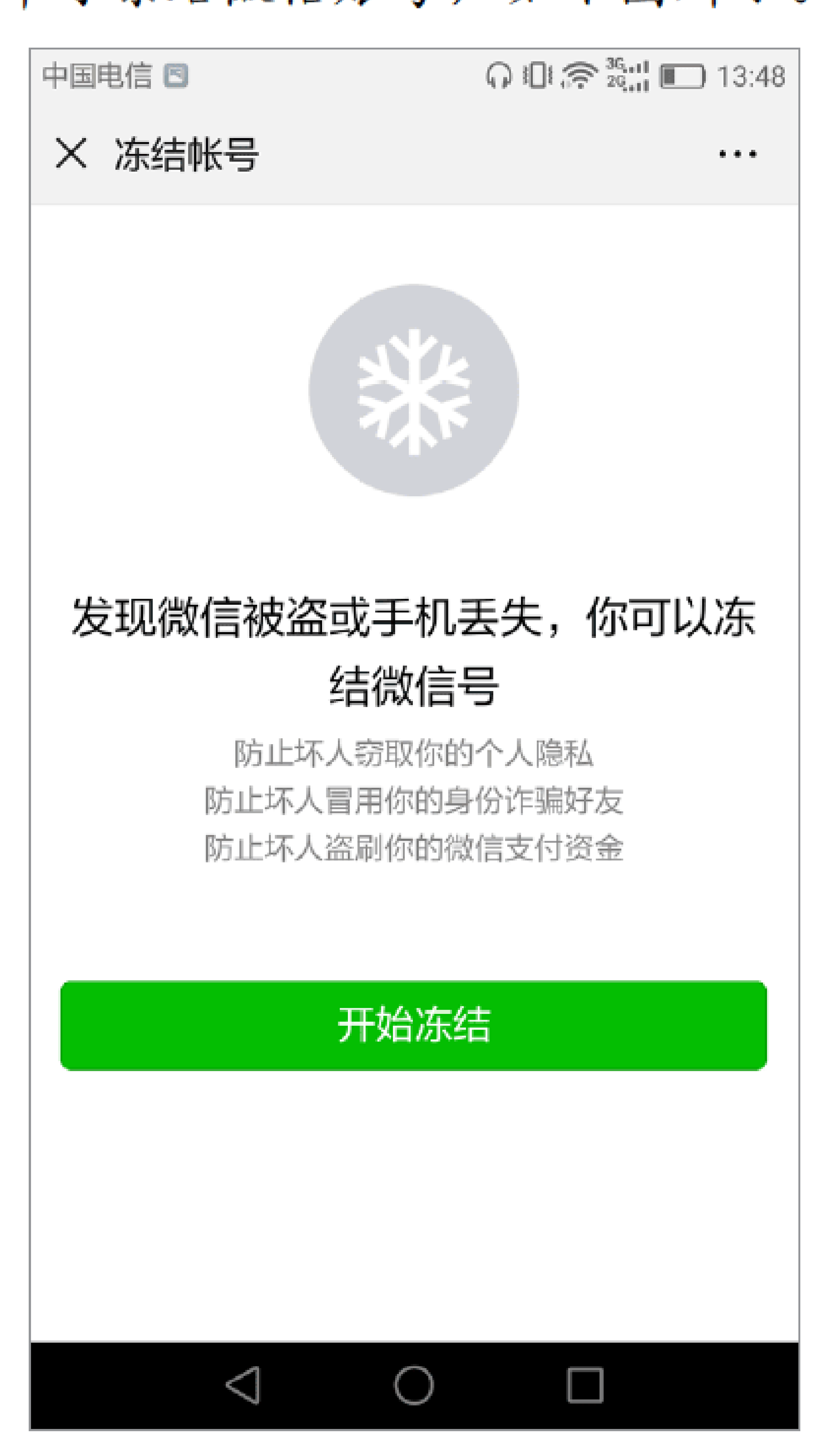




Step 04 点按“微信安全中心”选项，进入“微信安全中心”设置界面，如下图所示。



Step 05 点按“冻结账号”选项，进入“冻结账号”界面，在其中点按“开始冻结”按钮，即可冻结微信账号，如下图所示。



7.3　网银账号及密码的安全防护



网上银行为用户提供了安全、方便、快捷的网上理财服务，不仅使用户能够进行账户查询、支付结算等传统银行柜台服务，而且还可以实现现金管理、投资理财等功能。但是，为了保证网上银行的安全，一些安全措施是必不可少的。



实战7：网上挂失银行卡

当突然发现自己的银行卡丢失，则必须马上进行挂失。用户可以到实体银行申请挂失，也可以在网上申请挂失。在网上申请挂失的操作步骤如下。

Step 01 登录到自己的个人网上银行账户（这里以工商银行为例），在打开的页面中单击“网上挂失”按钮，进入“操作指南”页面，如下图所示。



Step 02 在“操作指南”页面中单击“挂失”链接，进入“挂失”页面，如下图所示。



Step 03 在其中输入要挂失的银行卡号，选择证件类型并输入证件号码，如下图所示。



Step 04 单击“挂失”按钮即可。

实战8：避免进入钓鱼网站

随着使用网上银行的用户越来越多，钓鱼网站也进入了一个“飞速”发展的阶段，用户一不小心就会进入黑客设计好的钓鱼网站，最后造成不可估量的损失。那么如何才能避免进入钓鱼网站呢？这就需要用户了解钓鱼网站的欺骗技术和防范钓鱼网站的方法。

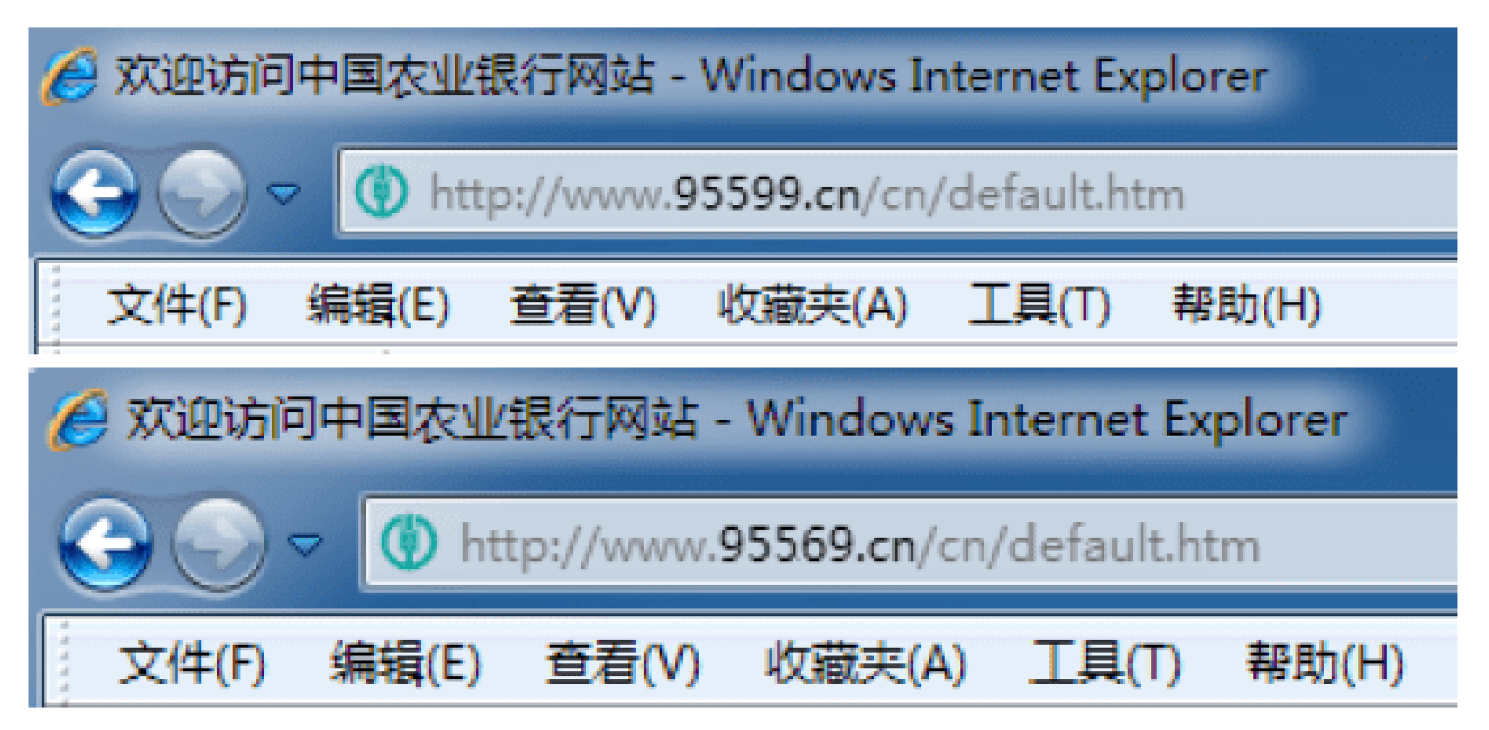
1. 网络钓鱼网站的欺骗技术

网络钓鱼的技术手段有多种，如邮件攻击、跨站脚本、网站克隆、会话截取等，但在各种网银事件中，最常见的是克隆网站和URL地址欺骗这两种手段，下面分别进行分析。

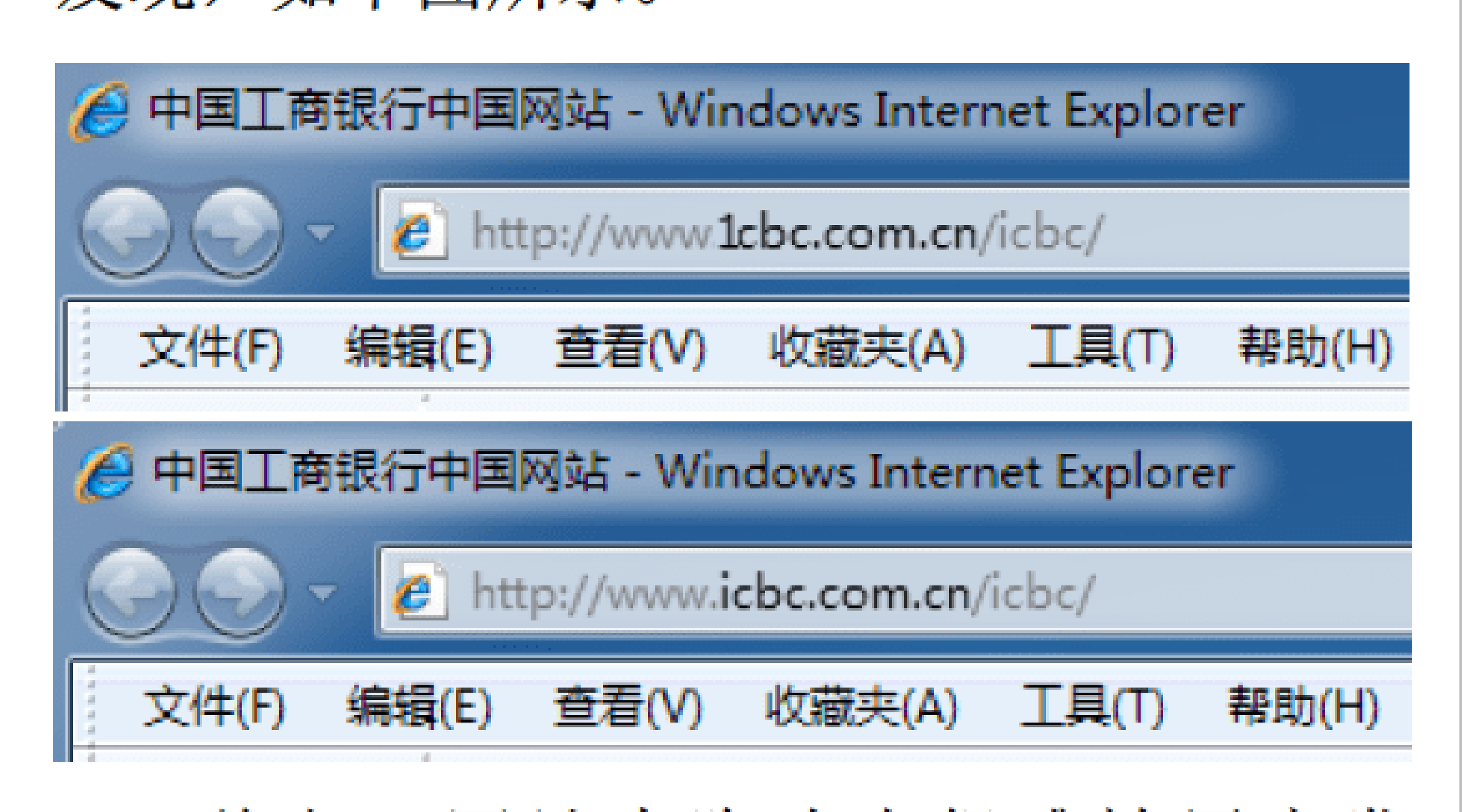
1）克隆网站

“克隆网站”，也称“伪造网站”，其攻击形式被称为域名欺骗攻击，即网站的内容和真实的银行网站非常相似，而且非常简单，最致命的一点是通过网站克隆技术克隆的网站和真实的网站真假很难辨别，有时只是在网站域名中有一些极细小的差别，不细心的用户就很容易上当。

进行网站克隆首先需要对网站的域名地址进行伪装欺骗，最常用的就是采用和真实银行的网址非常相似的域名地址，如虚假的农业银行域名地址为www.95569.cn，和真实的网址www.95599.cn只有一个“6”字之差，不细心的用户很难发现。如下图所示即为真实农业银行与虚拟农业银行的对比图。



另外，在其他银行中类似的情况也出现不少，如2004年出现的中国工商银行假冒的网站，使很多用户上当受骗，其假冒的网站域名为www.1cbc.com.cn，这与真实的网址www.icbc.com.cn只有数字“1”和字母i的不同。还有一些假冒的工商银行的网站地址www.icbc.com，只比真实的网址缺少cn两个字母，不细心的用户根本不容易发现，如下图所示。



总之，网站克隆攻击很难被用户发现，一不小心就很容易上当受骗。除此之外，现在网站的域名管理也不是很严格，普通用户也可以申请注册域名，使得网站域名欺骗屡屡发生，给网银用户带来了极大的经济损失。但是，假的真不了，真的假不了，即使伪造的网站页面无论是网站的Logo、图标、新闻和超级链接等内容都能连接到真实的网页，但在输入账号的位置处就会存在着与真实网站的不同之处，这是网站克隆攻击是否成功的关键所在。当用户输入自己的账号和密码时，网站会自动弹出一些不正常的窗口，如提示用户输入的账号或密码不正确，要求再次输入账号和密码的信息窗口等。其实，在用户第一次输入账号和密码并提示输入错误时，该账号信息已经被网站后门程序记录下来并发送到黑客手中了，如下图所示。



2）URL地址欺骗攻击

URL其全称为Uniform Resource Locators，即统一资源定位器的意思，在地址栏中输入的网址就属于URL的一种表达方式。基本上所有访问网站的用户都会使用到URL，其作用非常强大，但也可以利用URL地址进行欺骗攻击，即攻击者利用一定的攻击技术，构造虚假的URL地址，当用户访问该地址的网页时，以为自己访问的是真实的网站，从而把自己的财务信息泄漏出去，造成严重的经济损失。

在使用该方法进行诱骗时，黑客们常常是通过垃圾邮件或在各种论坛网页中发布伪造的链接地址，进而使用户访问虚假的网站。伪造虚假的URL地址的方

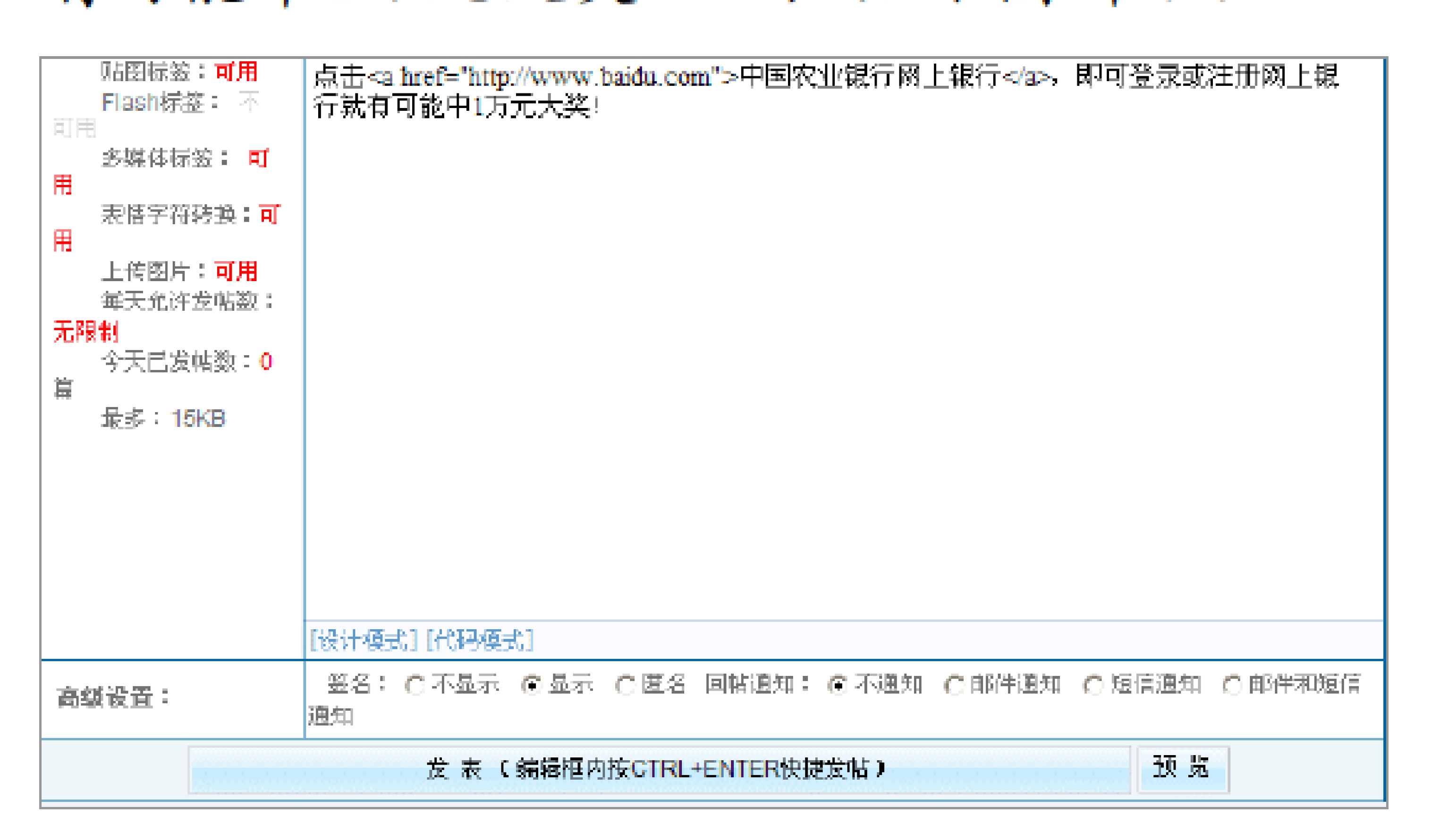
法有多种，如起个具有诱惑性的网站名称、掉包易混的字母数字等，但最常用的还是利用IE编码或IE漏洞进行伪造URL地址，该方法使用户单击的链接与真实的网址不符，从而登录到黑客伪造的网站中。

这里举一个具体的实例来说明利用URL伪造地址进行网上银行攻击的过程，具体的操作步骤如下。

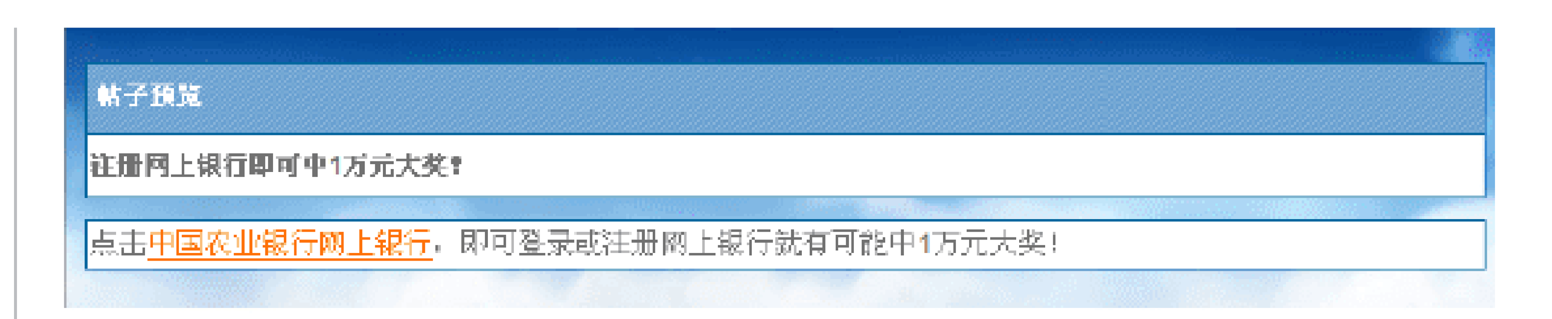
Step 01 在任意网上论坛中发布一个极具有诱惑性的帖子，其主题为“注册网上银行即可中1万元大奖！”，如下图所示。



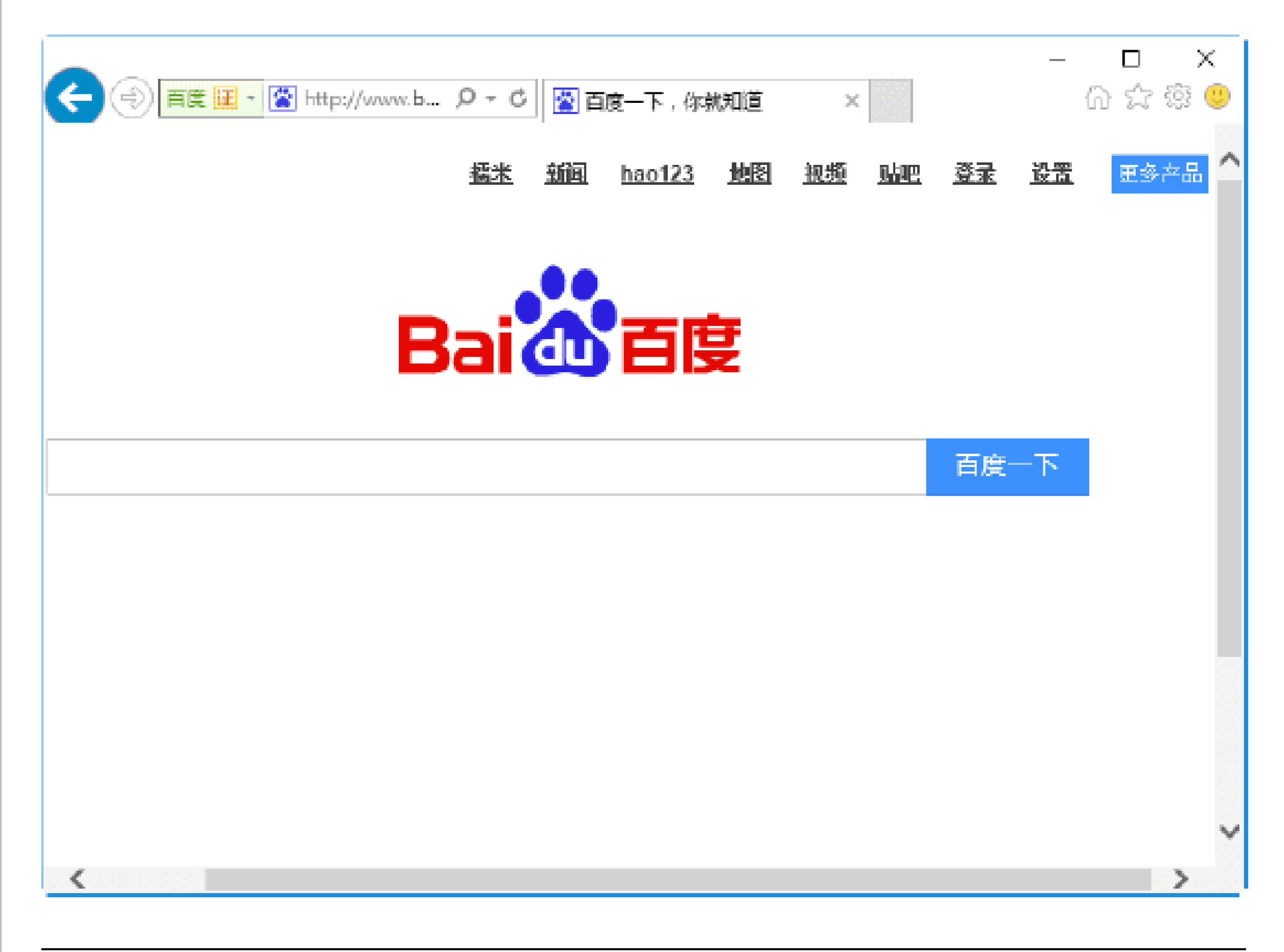
Step 02 在帖子内容中输入诱惑性的信息，并留下网上银行的链接地址，这个地址的作用是诱导用户登录到自己伪造的网站中，并使用户误认为自己登录的网站地址是正确的，因此需要在帖子中加入如下代码“点击中国农业银行网上银行，即可登录或注册网上银行就有可能中1万元大奖！”，如下图所示。



Step 03 输入完毕后，单击“发表”按钮或在编辑框内按快捷键Ctrl+Enter发表帖子。在帖子发表成功后，即可在网页中显示“中国农业银行网上银行”的信息，如下图所示。



Step 04 当用户单击“中国农业银行网上银行”链接时，打开的却是黑客伪造的网站，这里是百度网页，如下图所示。如果把百度的网址换成黑客伪造的银行网站，那么用户就有可能上当受骗。



提示： 当然，这种欺骗方法是一种比较简单的方法，稍有一点上网经验的用户只需将鼠标放置在超链接上，即可在下方的状态栏中看到实际所链接到的网址，从而识破该欺骗形式。

Step 05 为了进一步伪装URL地址，还需要在真实的网上银行URL地址中加入相关代码，如把上述帖子内容修改为“点击http://www.95599.cn/ ，即可登录或注册网上银行就有可能中1万元大奖！”，如下图所示。



Step 06 发帖成功后，在网页中将显示http://www.95599.cn的链接地址，即使鼠标移动

到链接地址上，在其窗口的状态栏中看起来依然链接到http://www.95599.cn。但是到单击该链接后才发现打开的是伪装的网站，如下图所示。



总之，针对上述情况，用户在上网的过程中，一定要随时注意地址栏中URL的变化，一旦发现地址栏中的域名发生变化，就要引起高度的重视，从而避免自己上当受骗。

3）浏览器漏洞攻击

利用浏览器的相关漏洞和语法错误等，可以让用户无法觉察到URL地址的变化，进而起到欺骗用户的目的。如在一些没有打过补丁的计算机中，将URL地址修改为http://www.95599.cn/@www.baidu.com/，当用户单击后，在打开的浏览器标题栏和地址栏中都会看到其链接地址为http://www.95599.cn，但其实际上显示的页面却是百度网页。



这时如果将百度网址换成黑客伪造的银行地址，后果是十分严重的。另外，URL欺骗攻击的手段还有其他形式，如利用IE最新漏洞或其他一些脚本编程技术，使得新打开的网页不显示地址栏或完全显示与真实网站页面一样的信息。所以，网上银行使用者一定要及时为自己的系统打上漏洞补丁，以避免黑客们利用这个漏洞来窃取自己的银行账户等隐私信息。

实战9：使用网银安全证书



网银安全证书是银行系统为网银客户提供的一种高强度的安全认证产品，也是网银用户登录网上银行系统的唯一凭证。目前，所有国内银行网站，在第一次进入网银服务项目时，都需要下载并安装安全证书，所以网银用户可以通过检查网银安全证书，来确定打开的银行网站系统是不是黑客伪造的。这里以中国工商银行为例，具体介绍一下网银安全证书下载并安装的过程，进而判断自己打开的银行网站的真伪，具体的操作步骤如下。

Step 01 在IE浏览器地址栏中输入工商银行的网址http://www.icbc.com.cn，打开该银行系统的首页，在该页面的左侧单击网上银行任意服务项目按钮，即可打开该服务项目的账号密码登录页面，如单击“个人网上银行登录”按钮，即可打开“个人网上银行登录”窗口，如下图所示。



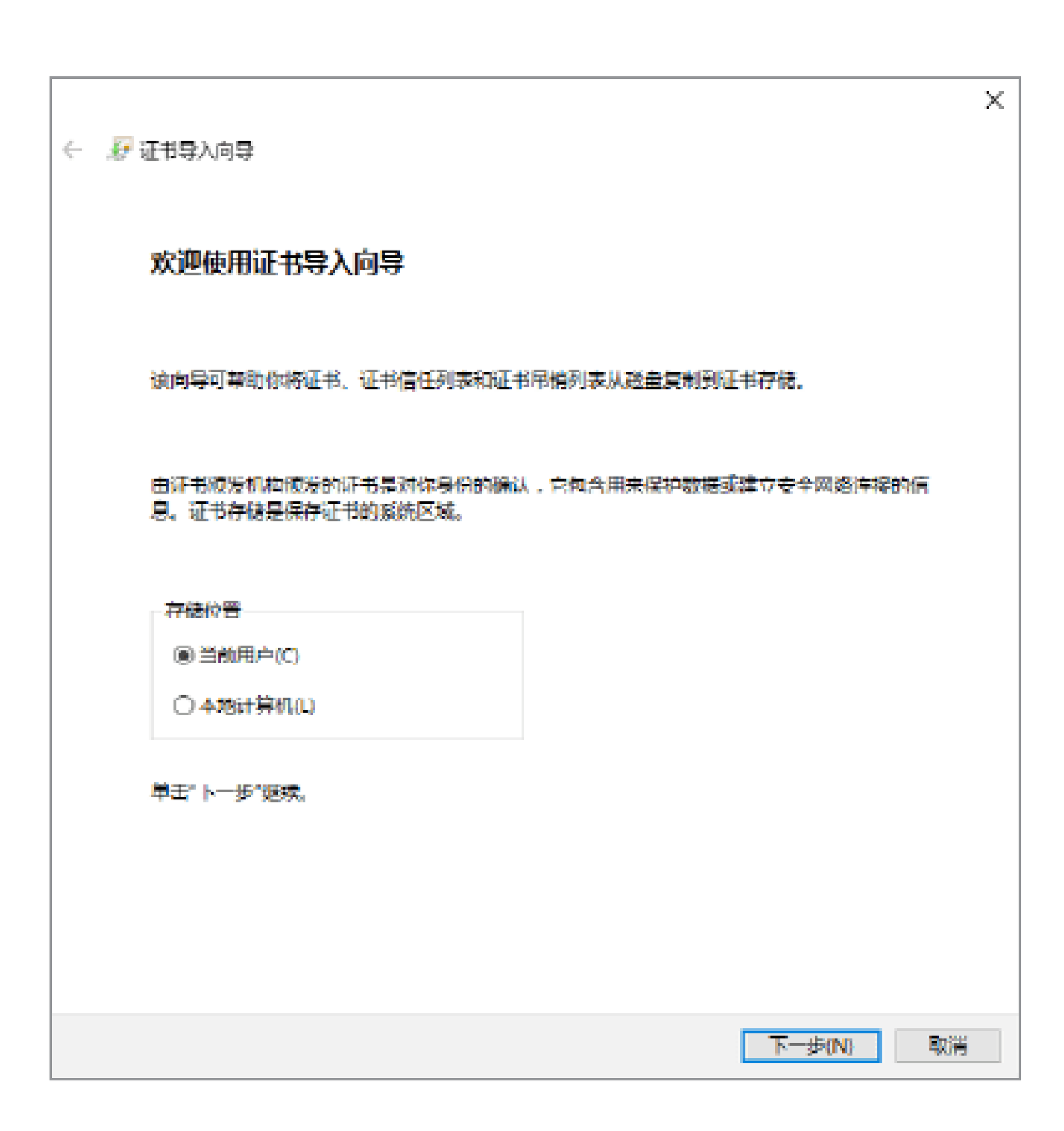
Step 02 在该登录页面地址栏后面可看到一个图标按钮，单击该按钮即可弹出“网站标识”信息提示页面，提示用户本次与服务器的连接是加密的，如下图所示。



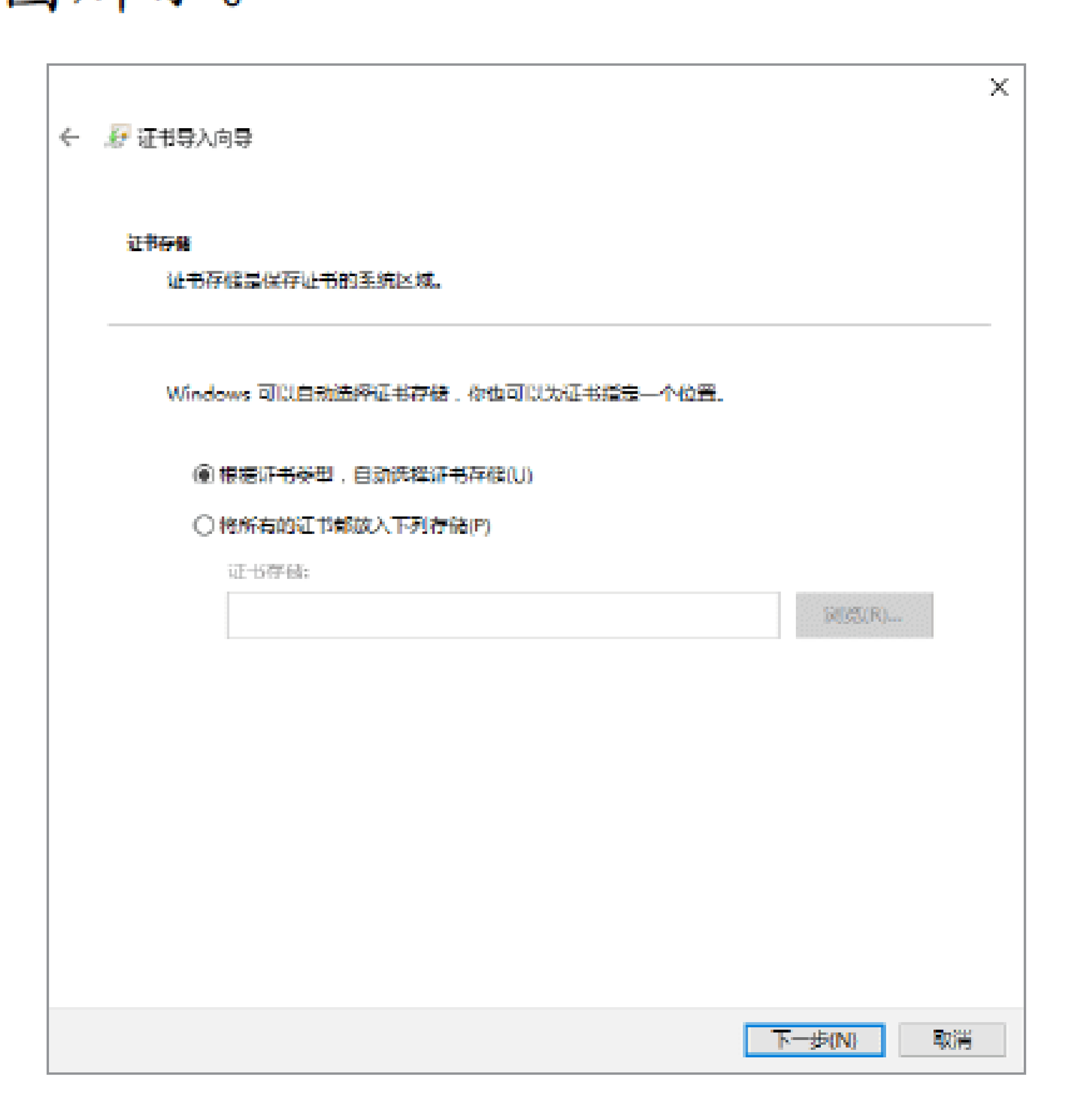
Step 03 单击“查看证书”连接按钮，打开“证书”对话框，在“常规”选项卡中可查看该证书的目的、颁发给、颁发者和有效起始日期等信息，如下图所示。



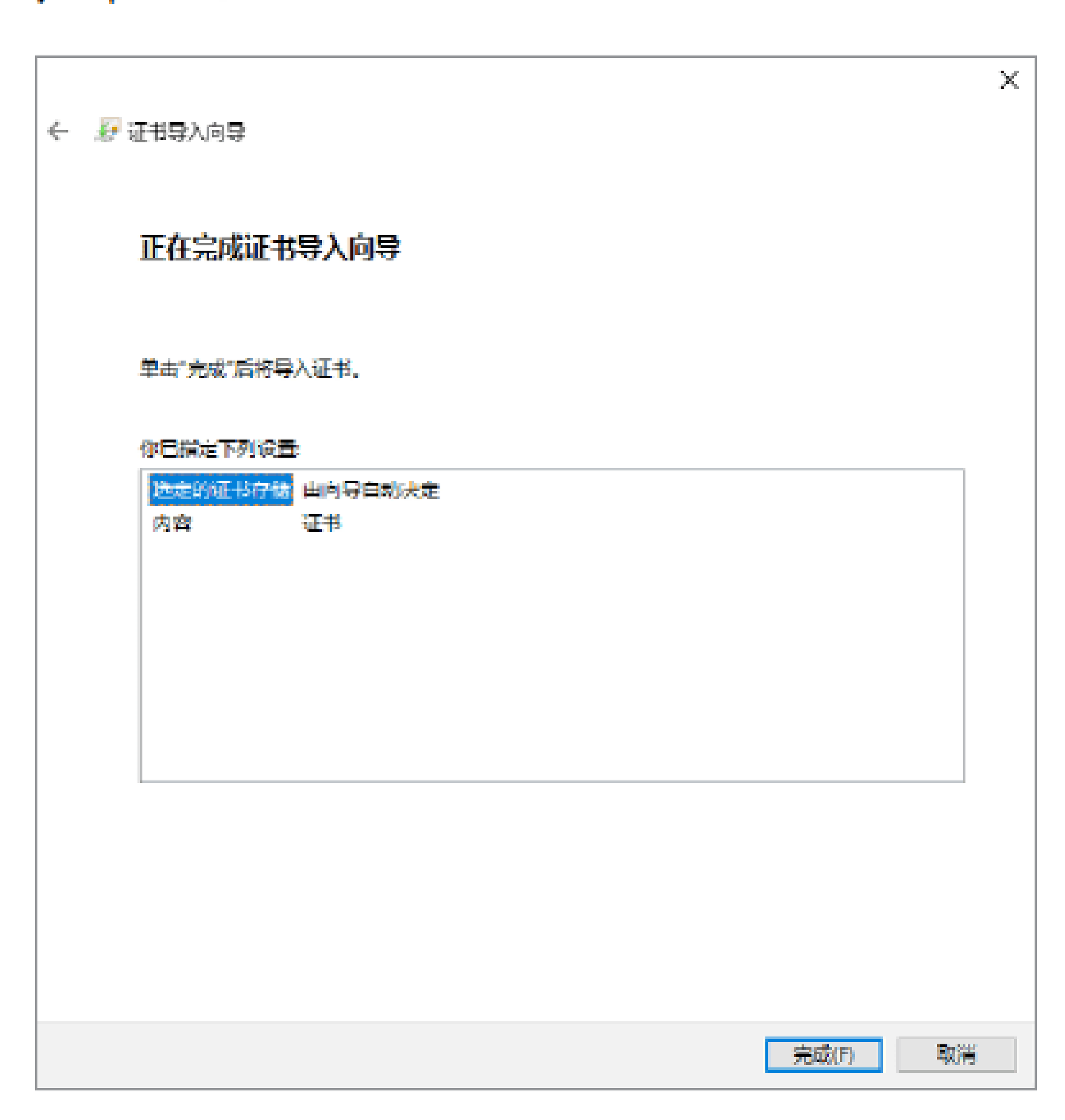
Step 04 单击“安装证书”按钮，打开“欢迎使用证书导入向导”对话框，如下图所示。该向导将帮助网银用户把证书、证书信任列表和证书吊销列表从磁盘中复制到证书存储区中。



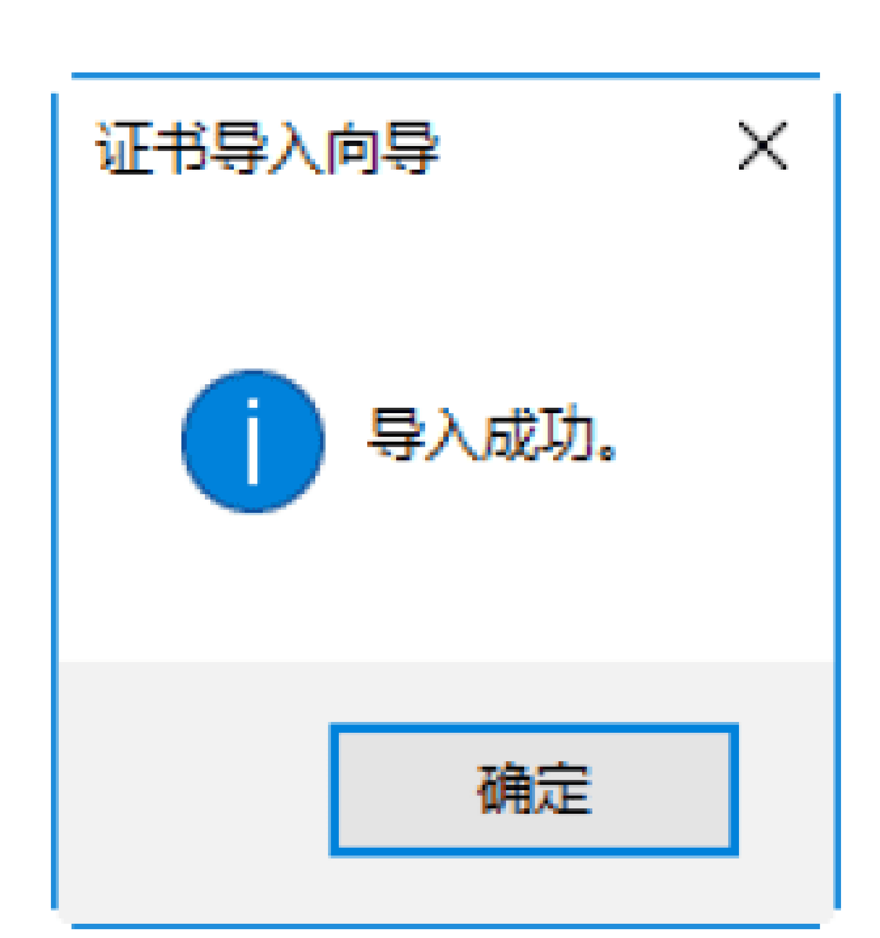
Step 05 单击“下一步”按钮，打开“证书存储”对话框，其中证书存储区是保存证书的系统区域，用户可根据实际需要自动选择证书存储区，一般采用系统默认选项“根据证书类型，自动选择证书存储”，如下图所示。



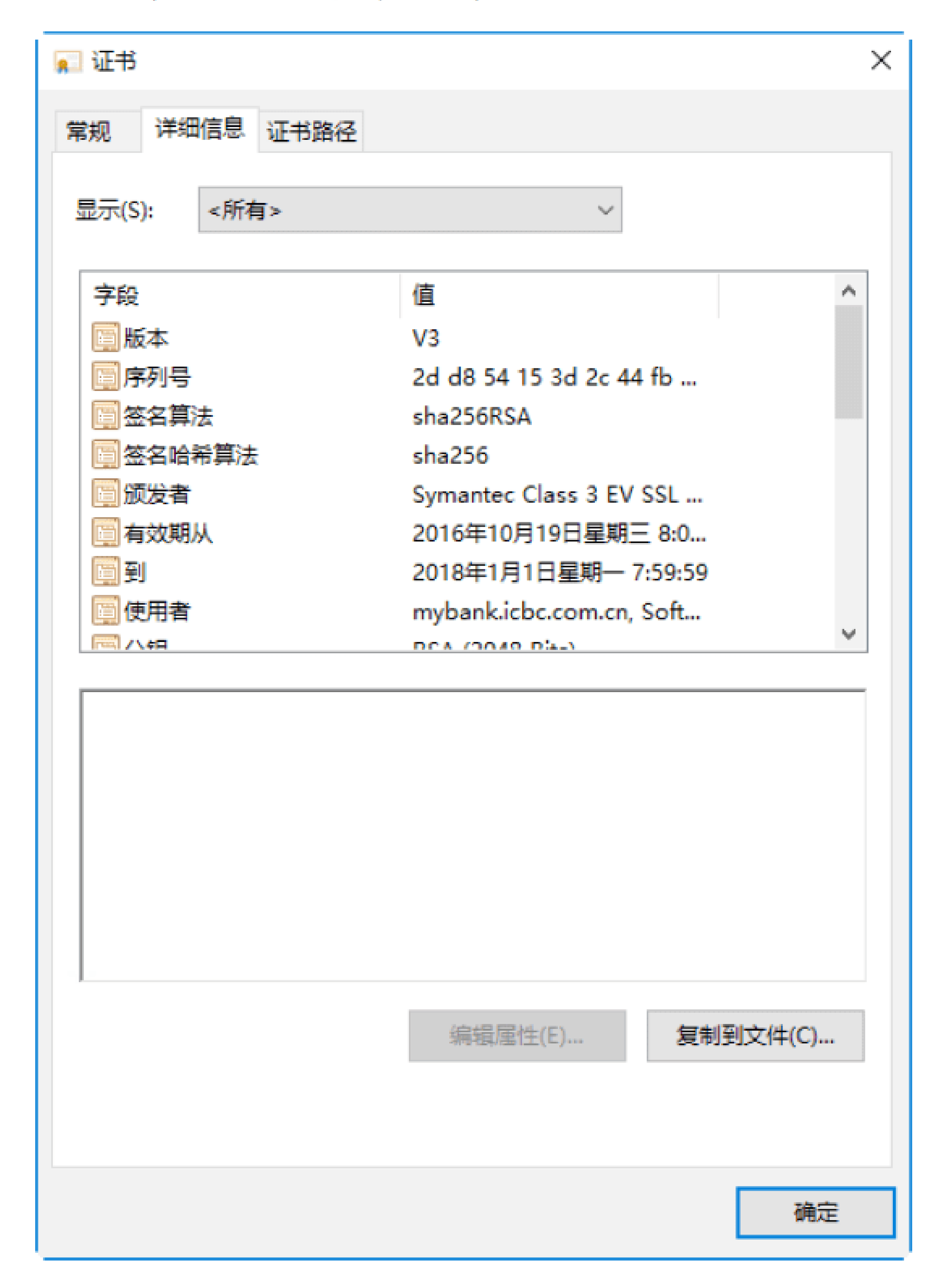
Step 06 选择完毕，单击“下一步”按钮，即可打开“正在完成证书导入向导”对话框，并提示用户已成功完成证书的导入，如下图所示。



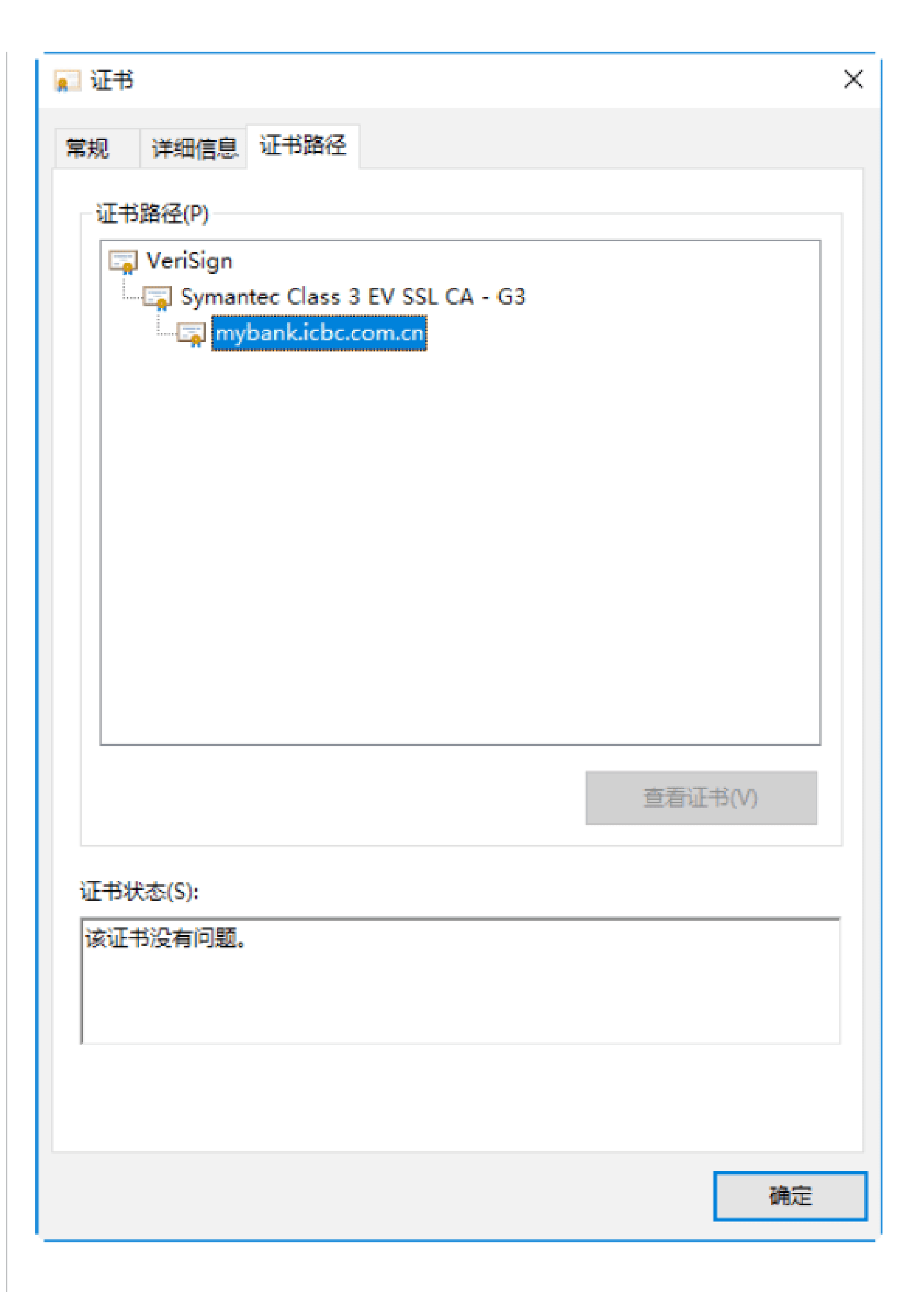
Step 07 单击“完成”按钮，打开“导入成功”对话框，如下图所示。至此，就完成了中国工商银行网上银行安全证书的安装操作。



Step 08 切换到“详细信息”选项卡，即可在该界面中根据实际需要查看证书的相关信息，如证书的版本、序列号、主题、公钥、算法、证书策略等，如下图所示。



Step 09 切换到“证书路径”选项卡，即可在该界面中查看证书的相关路径信息，如下图所示。



提示：在网银安全证书安装完毕之后，就可以使用该证书来保护自己的网银账号安全了。注意在查看网银证书信息时，一定要注意网银证书上的信息是否正确以及证书是否在有效期内，如果证书显示的信息不一致或不在有效期内，那么这个网上银行系统就有可能是黑客伪造的钓鱼网站。

7.4　实战演练

实战演练1——使用手机钱包给手机充话费



使用手机钱包可以给手机号充值，具体操作步骤如下。

Step 01 在手机微信中进入“我”界面，在其中可以看到“钱包”选项，如下图所示。



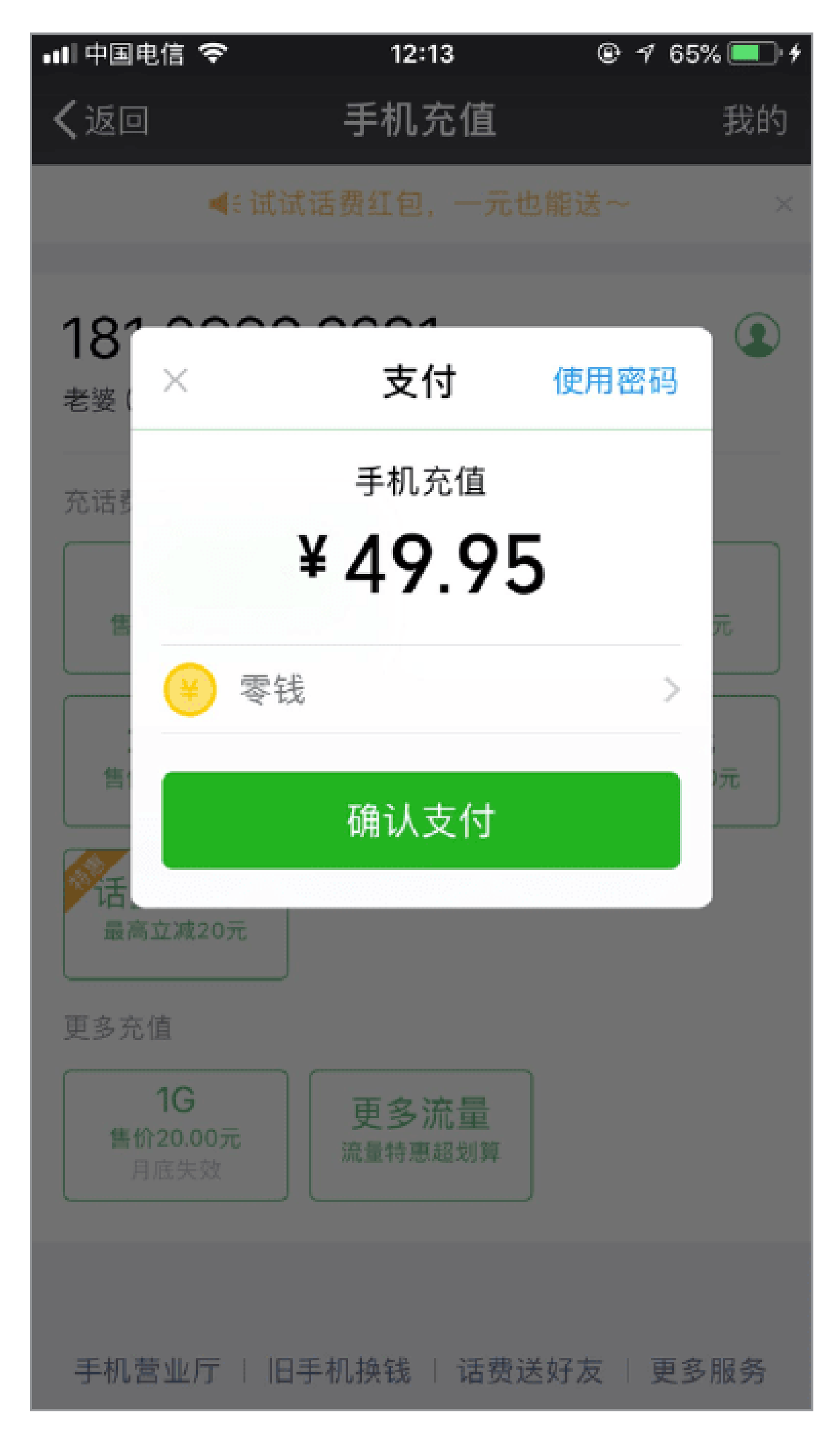
Step 02 点按“钱包”选项，进入“钱包”设置界面，可以看到当前钱包中的零钱以及服务项目，如下图所示。



Step 03 点按“手机充值”选项，进入“手机充值”界面，在其中输入手机号码，如下图所示。



Step 04 点按需要充值的金额，如这里点按50元，会弹出“支付”界面，点按“确认支付”按钮，即可完成使用钱包充值话费的操作，如下图所示。

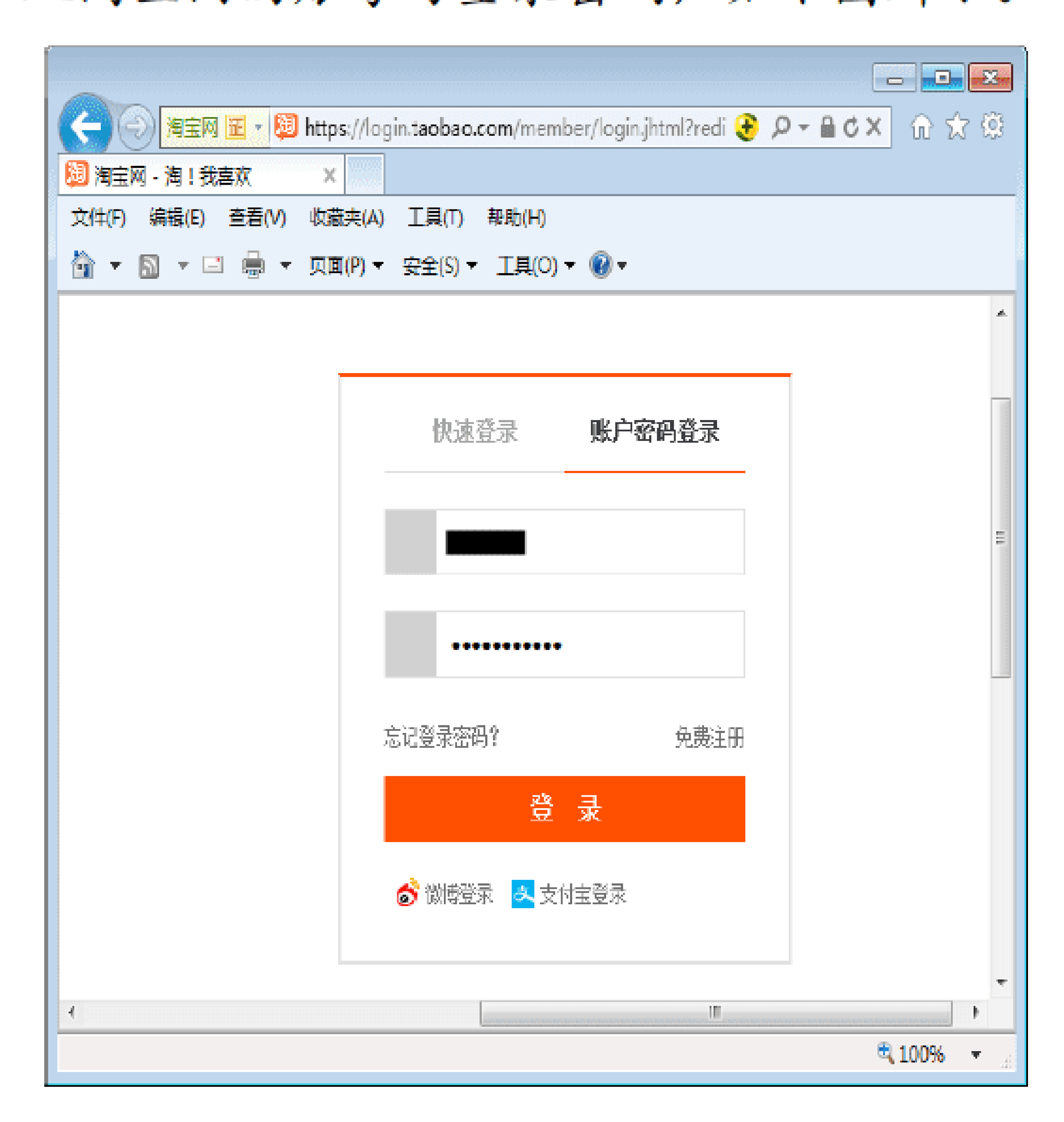


实战演练2——使用网银进行网上购物

网上购物，就是通过互联网检索商品信息，并通过电子订购单发出购物请求，然后进行网上支付，厂商通过邮购的方式发货，或是通过快递公司送货上门。这里以在淘宝上购物为例，介绍使用网上银行进行购物的方法。

要想在淘宝网上购买商品，首先要注册一个账号，才可以以淘宝会员的身份在其网站上进行购物。下面介绍如何在淘宝网上注册会员并购买物品。

Step 01 打开淘宝网用户登录界面，在其中输入淘宝网的账号与登录密码，如下图所示。

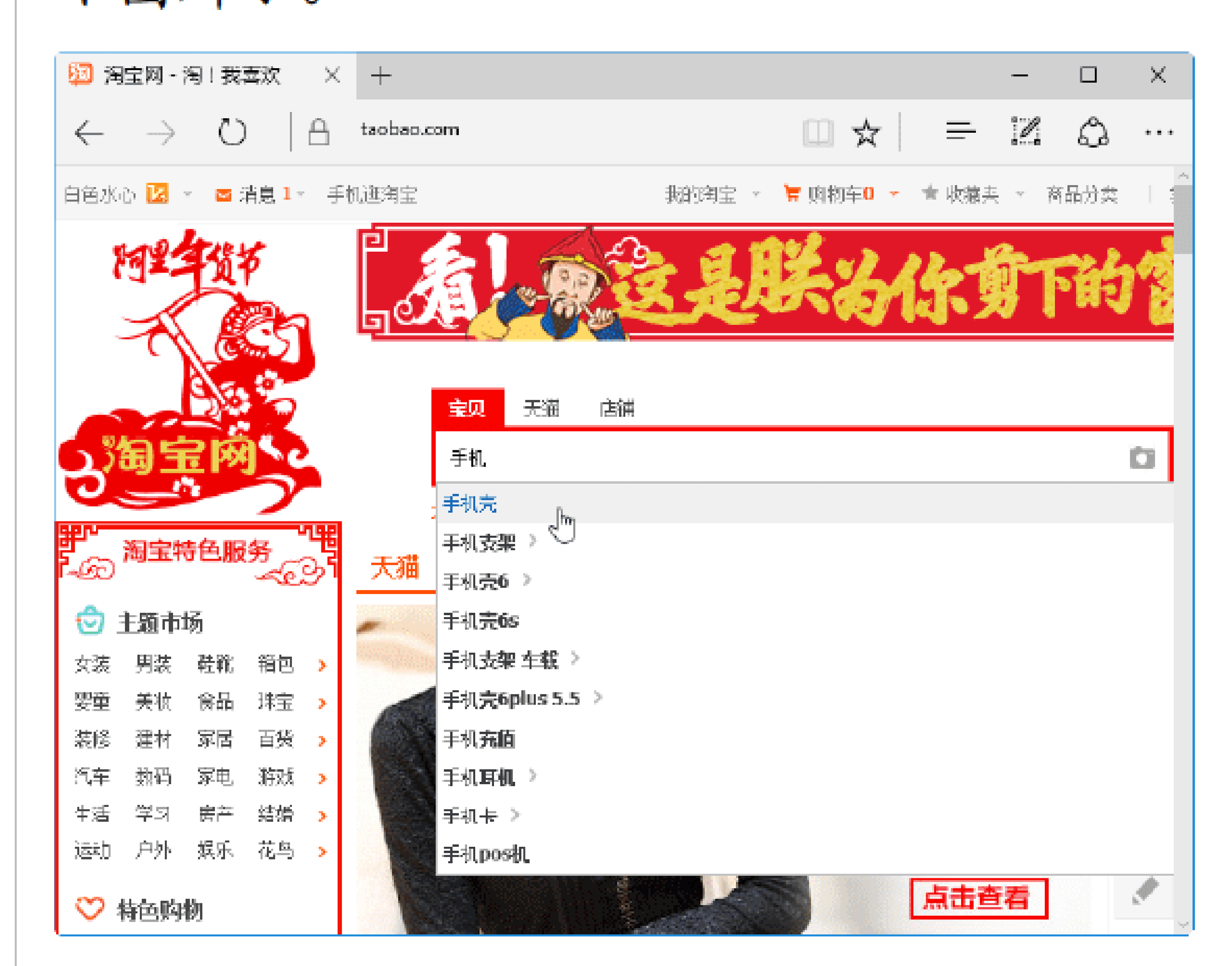


Step 02 单击“登录”按钮，即可以会员的身份登录淘宝网，这时在淘宝网首页的左上角显示登录的会员名，如下图所示。

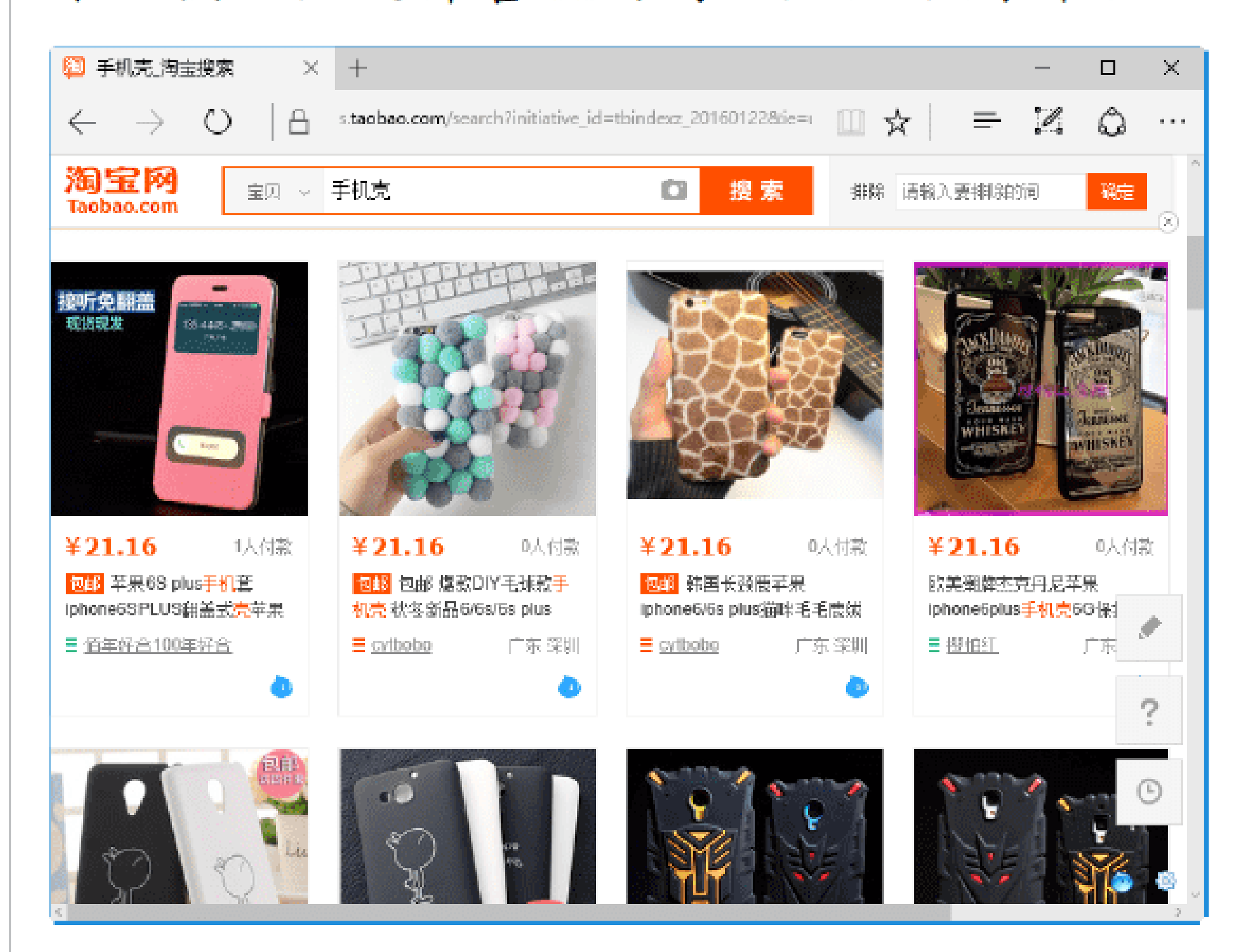




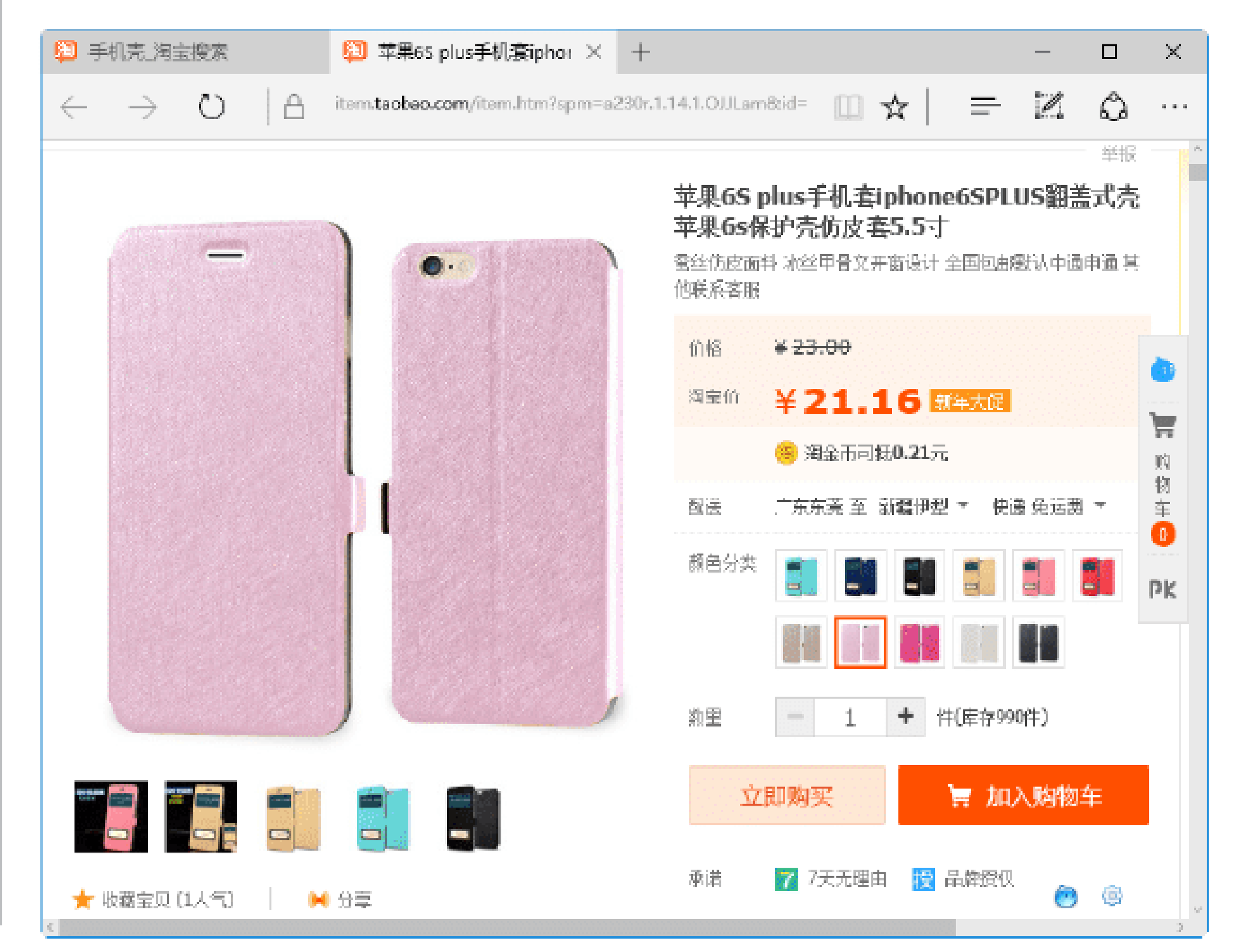
Step 03 在淘宝网的首页搜索文本框中输入自己想要购买的商品名称，如这里想要购买一个手机壳，就可以输入“手机壳”，如下图所示。



Step 04 单击“搜索”按钮，弹出“搜索结果”页面，选择喜欢的商品，如下图所示。

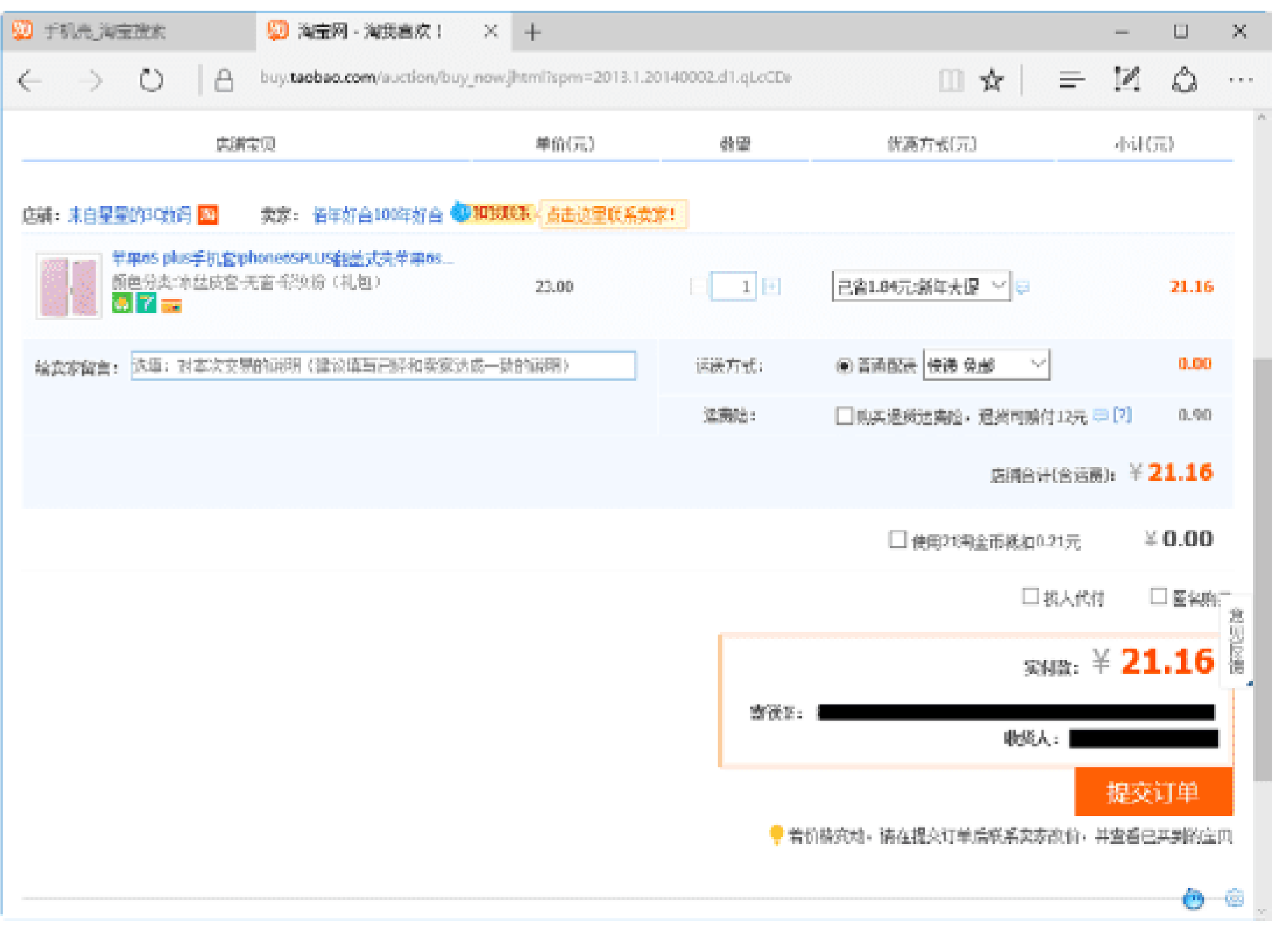


Step 05 单击其图片，弹出商品的详细信息页面，在“颜色分类”中选择商品的颜色分类，并输入购买的数量，如下图所示。

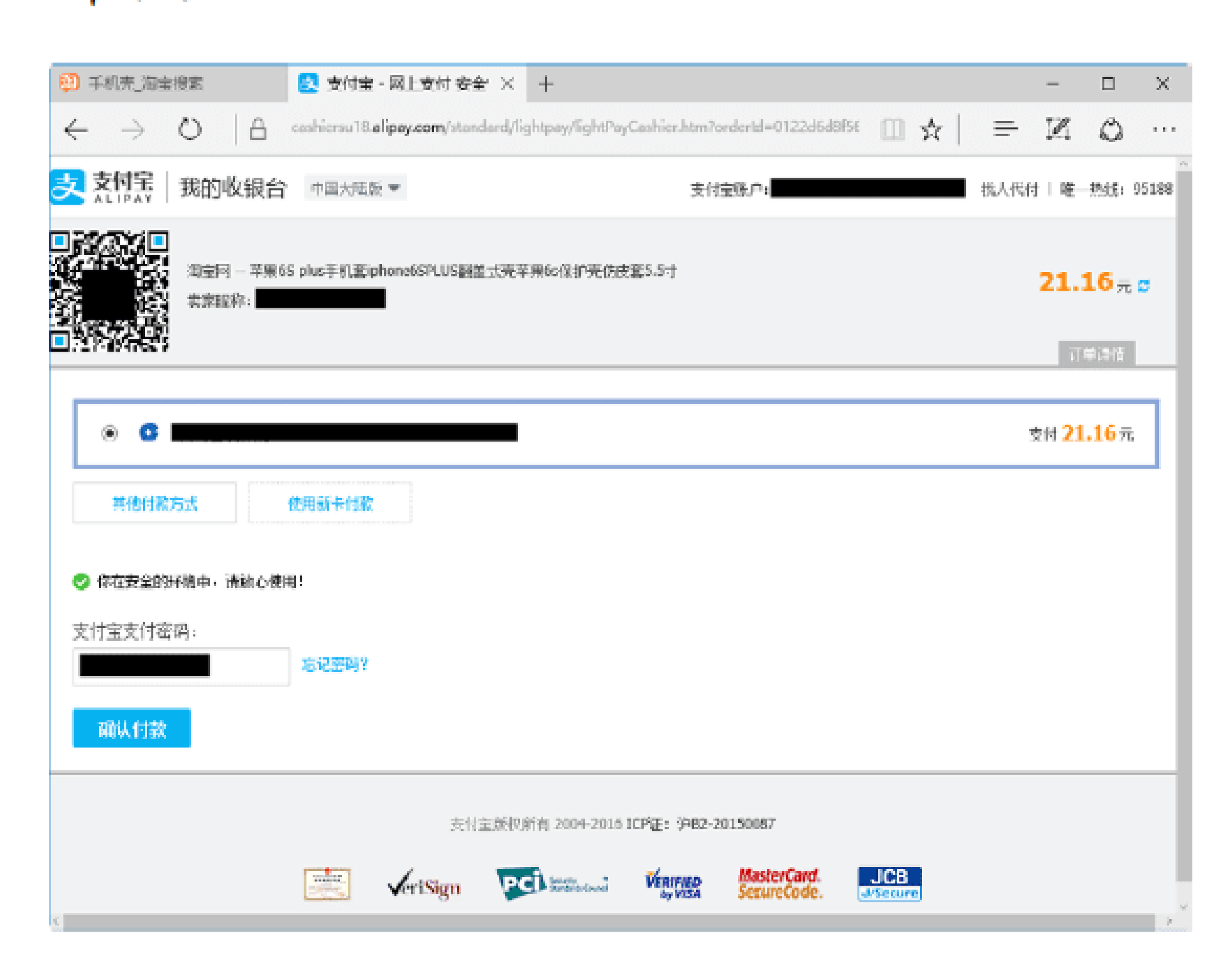




Step 06 单击“立刻购买”按钮，弹出“发货详细信息”页面，设置收货人的详细信息和运货方式，单击“提交订单”按钮，如下图所示。



Step 07 弹出支付宝“我的收银台”窗口，在其中输入支付宝的支付密码，如下图所示。



Step 08 单击“确认付款”按钮，即可完成整个网上购物操作，并在打开的界面中显示付款成功的相关信息，接下来只需要等待快递送货即可，如下图所示。



7.5　小试身手

练习1：启动系统中的BitLocker功能

对磁盘数据进行加密可以使用Windows 10操作系统中的BitLocker功能，该功能主要用于解决用户数据的失窃、泄漏等安全性问题。

使用BitLocker加密磁盘数据之前，需要启动BitLocker功能，具体的操作步骤如下。

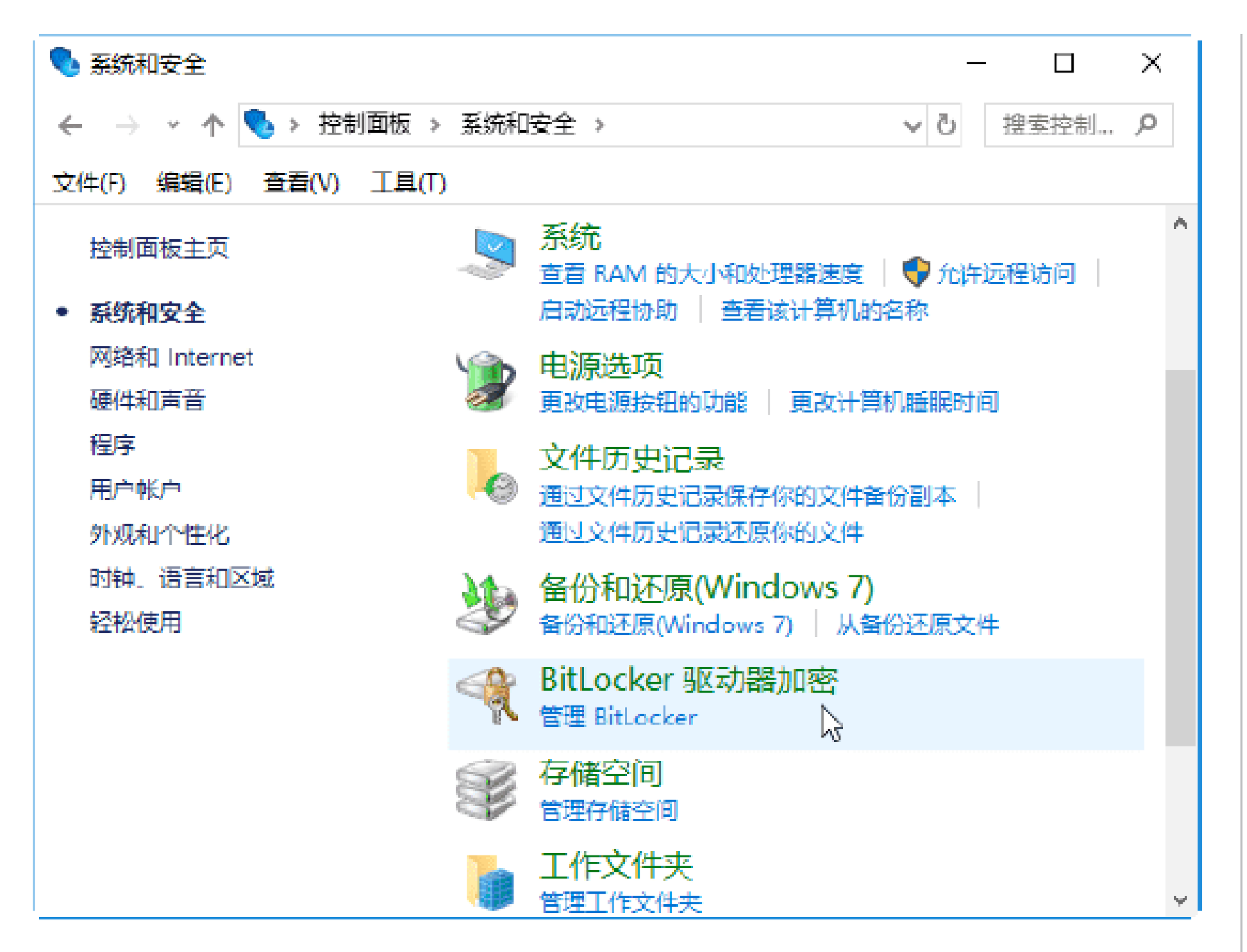
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“控制面板”选项，如下图所示。



Step 02 打开“控制面板”窗口，如下图所示。



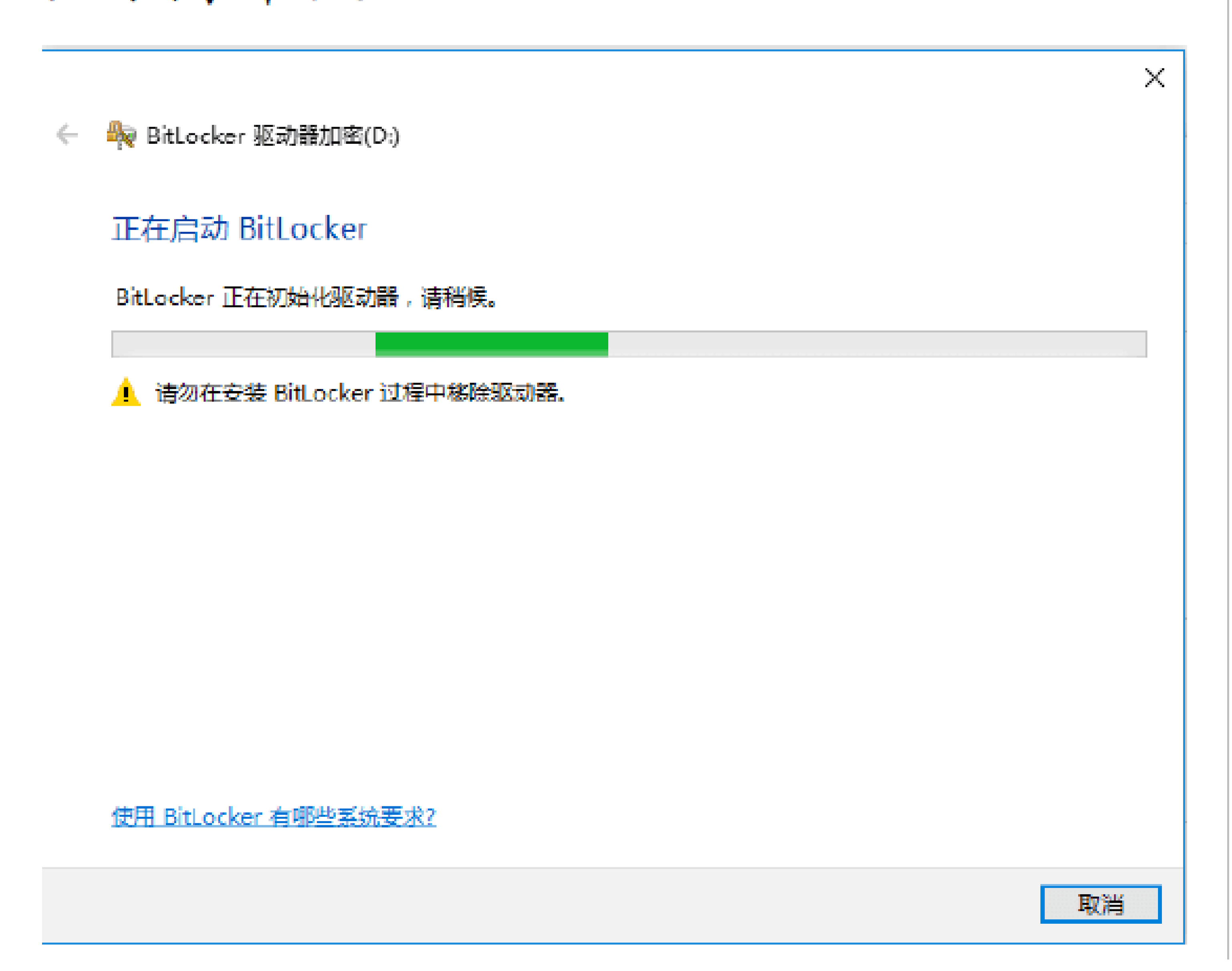
Step 03 在“控制面板”窗口中单击“系统和安全”链接，打开“系统和安全”窗口，如下图所示。



Step 04 在该窗口中单击“BitLocker驱动器加密”链接，打开“BitLocker驱动器加密”窗口，在窗口中显示出可以加密的驱动器盘符和加密状态，展开各个盘符后，单击盘符后面的“启用BitLocker”链接，对各个驱动器进行加密，如下图所示。



Step 05 单击D盘后面的“启用BitLocker”链接，打开“正在启动BitLocker”对话框，如下图所示。



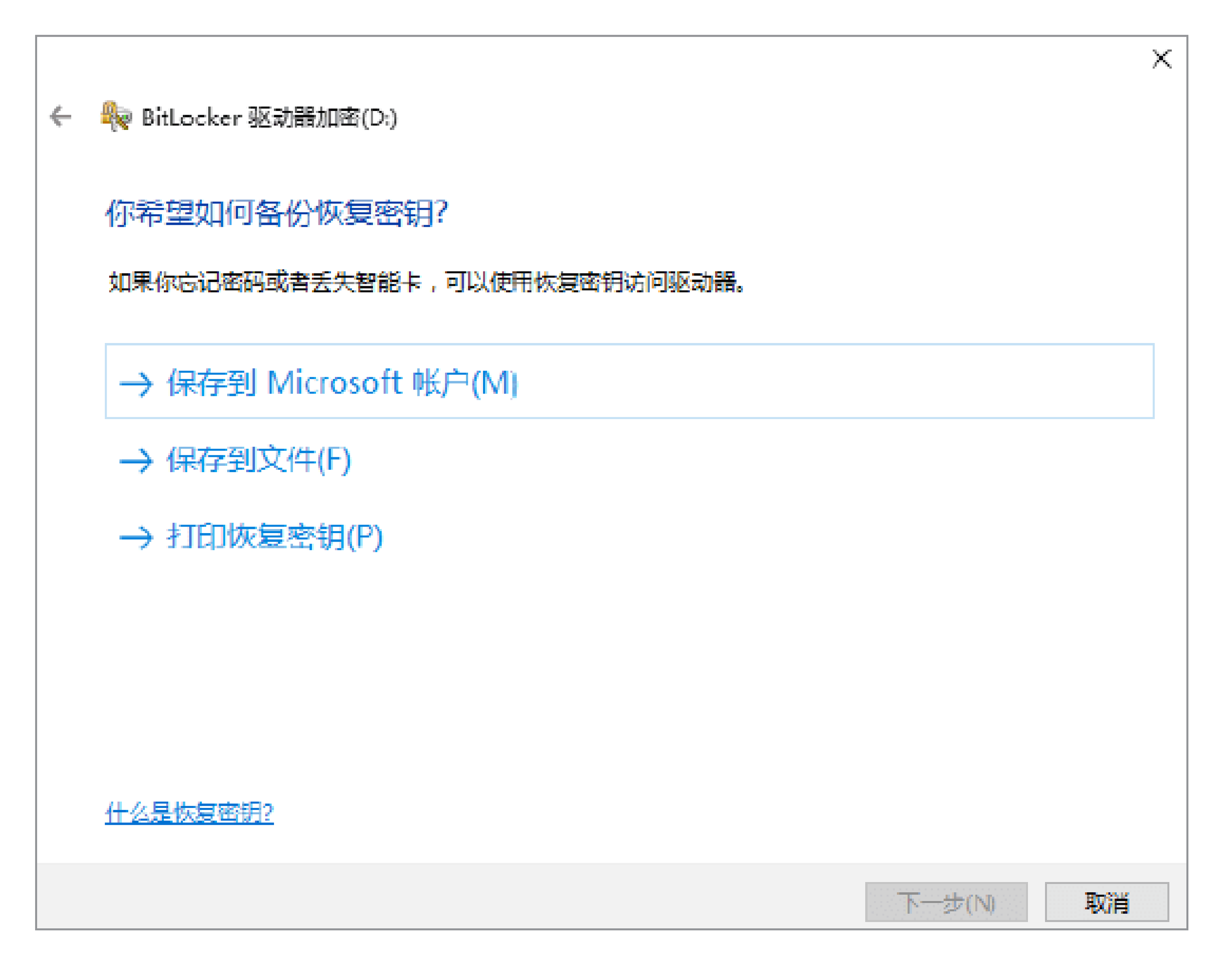
练习2：使用BitLocker功能加密磁盘数据

启动BitLocker完成后，下面就可以为磁盘数据进行加密操作了，具体的操作步骤如下。

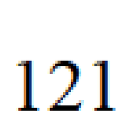
Step 01 启动BitLocker完成后，打开“选择希望解锁此驱动器的方式”对话框，勾选“使用密码解锁驱动器”复选框，按要求输入内容，如下图所示。

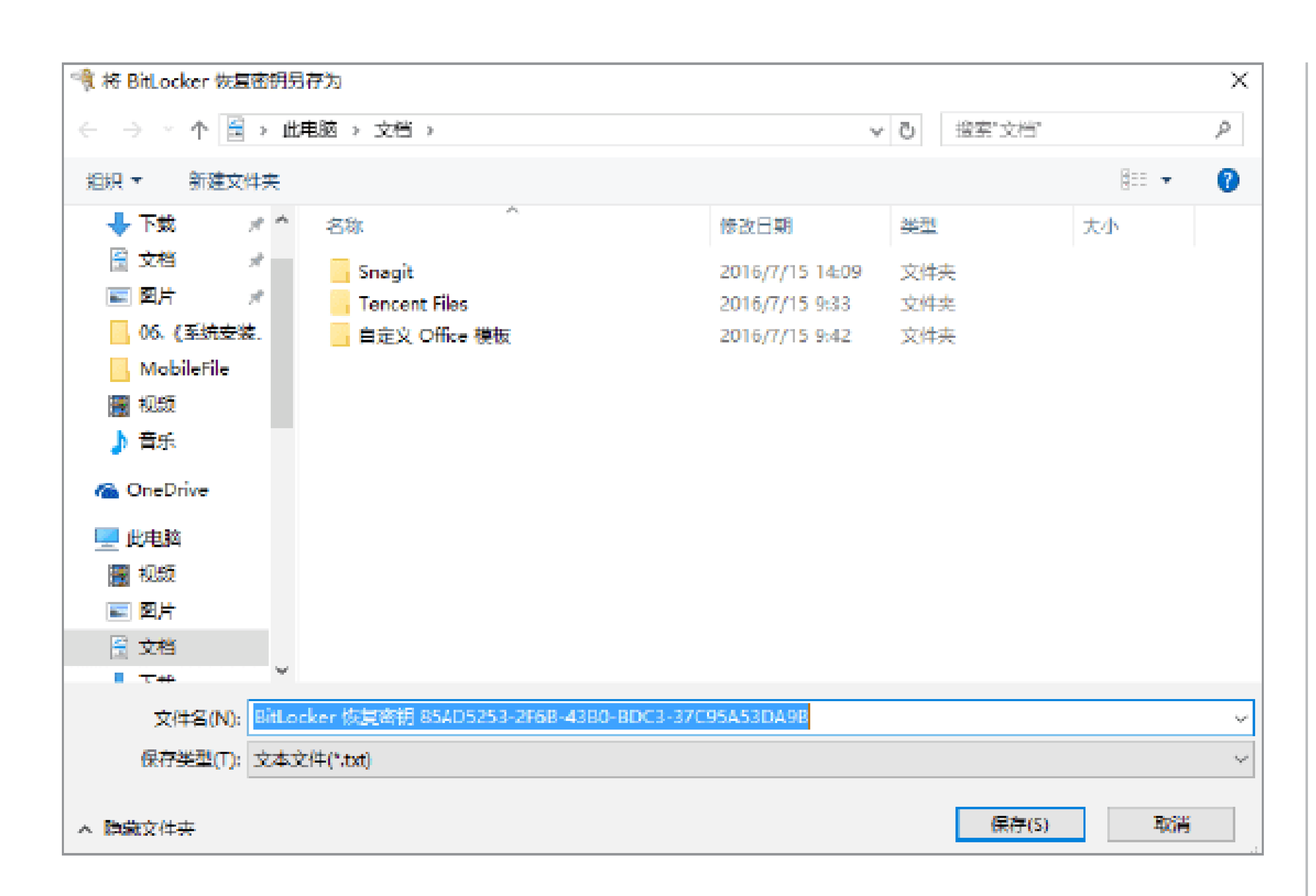


Step 02 单击“下一步”按钮，打开“你希望如何备份恢复密钥”对话框，可以选择“保存到Microsoft账户”“保存到文件”和“打印恢复密钥”选项，这里选择“保存到文件”选项，如下图所示。

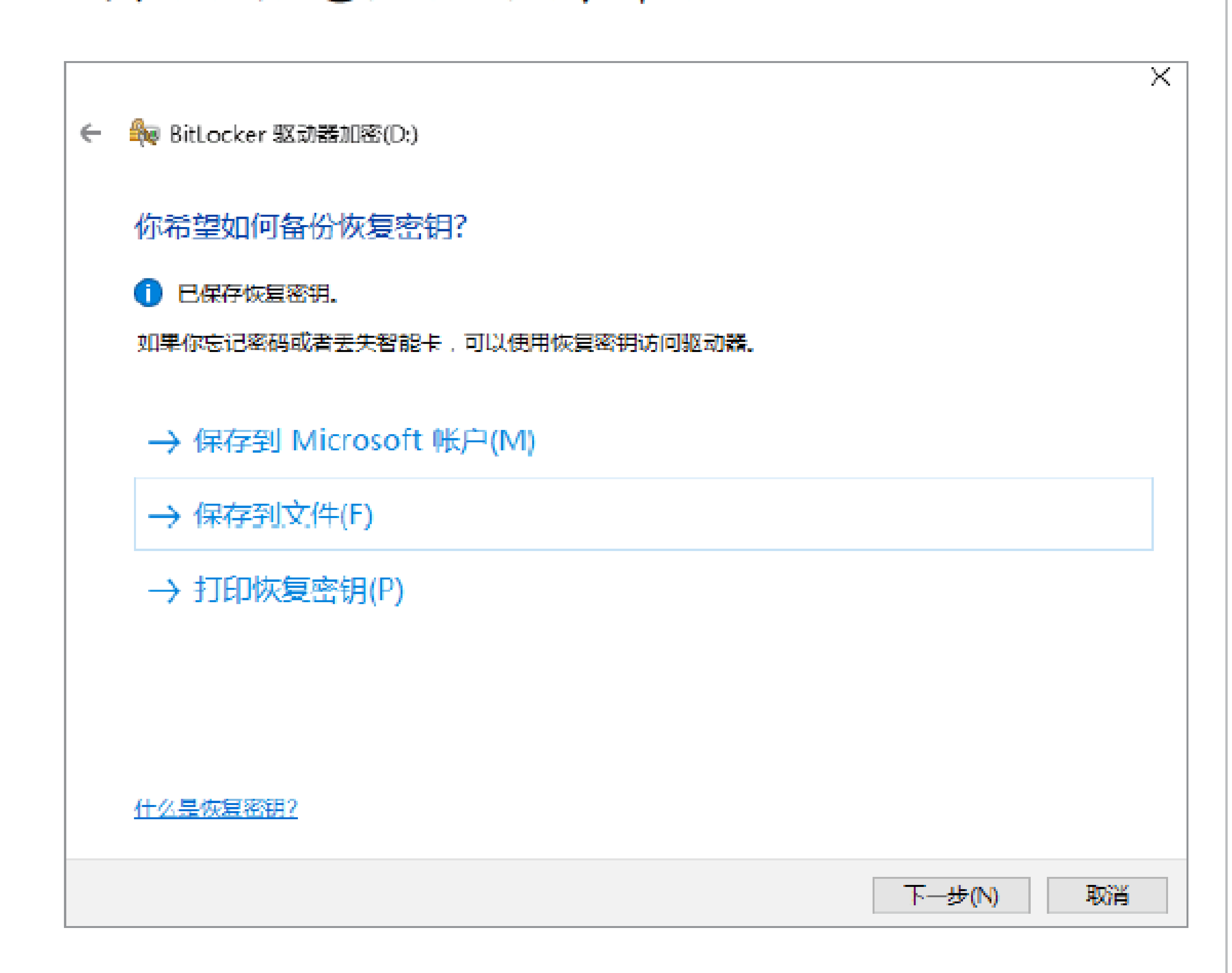


Step 03 打开“将BitLocker恢复密钥另存为”对话框，本窗口选择恢复密钥保存的路径，在文件名文本框中更改文件的名称，如下图所示。

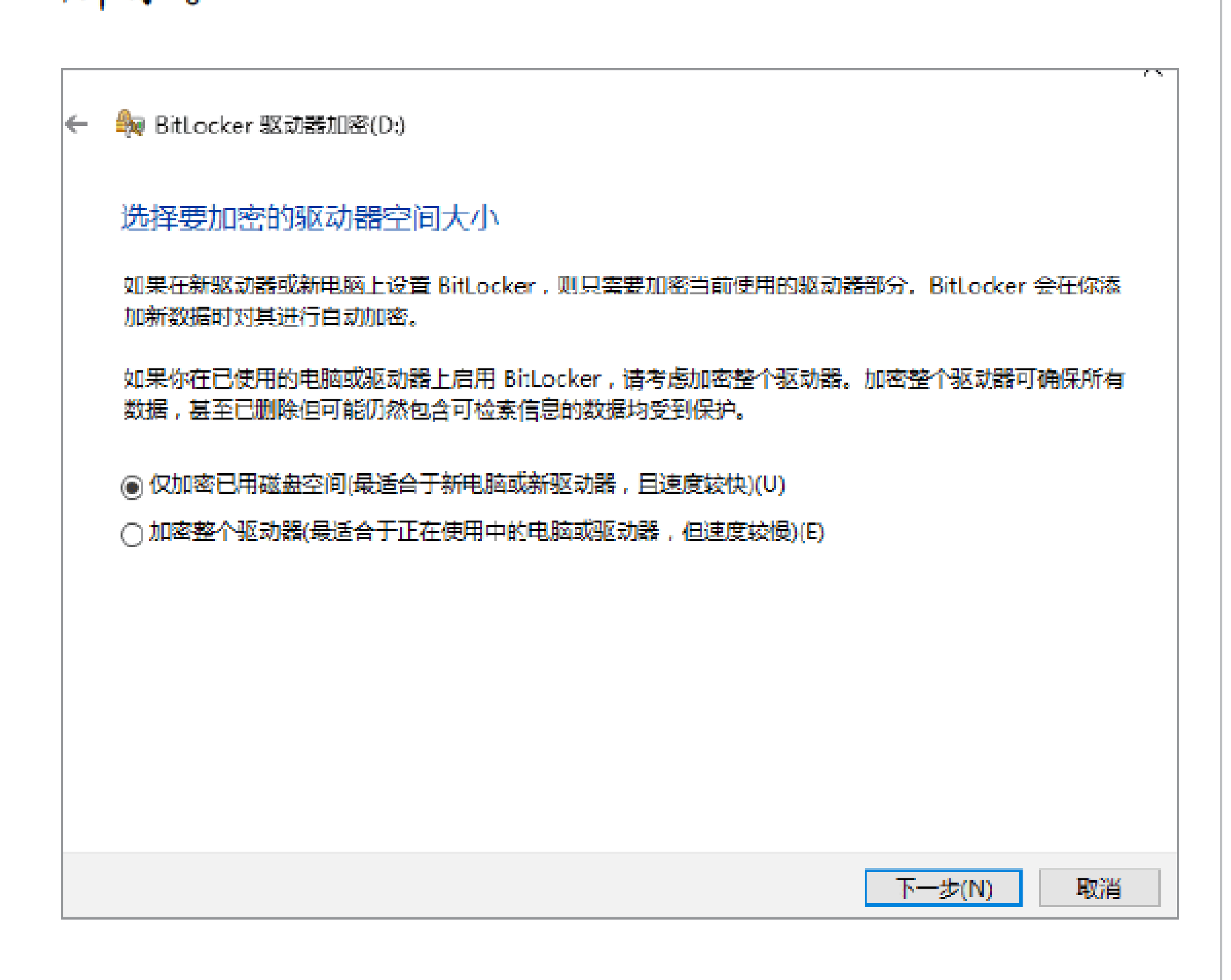




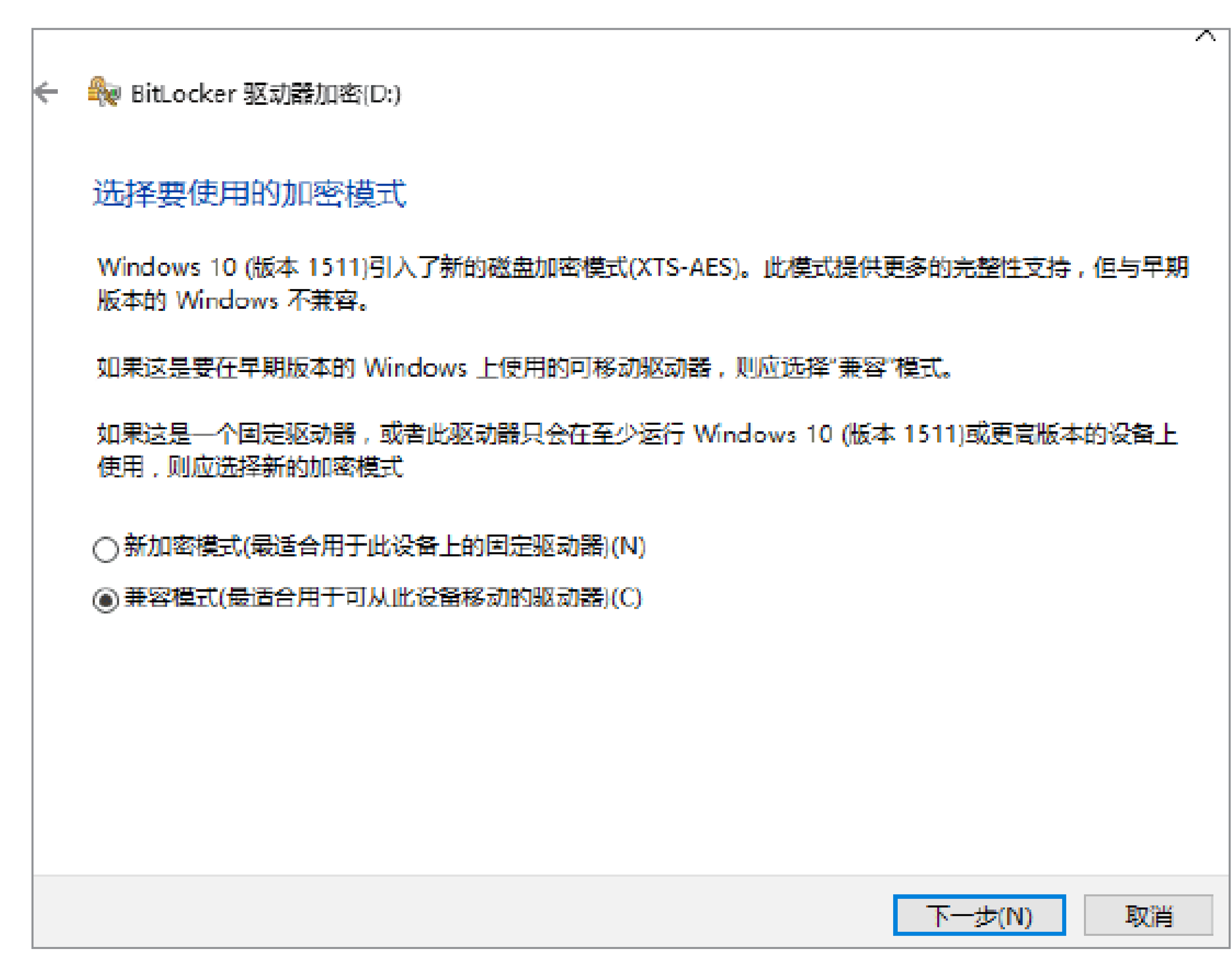
Step 04 单击“保存”按钮，关闭对话框，返回“你希望如何备份恢复密钥”对话框，在对话框的下侧显示“已保存恢复密钥”的提示信息，如下图所示。



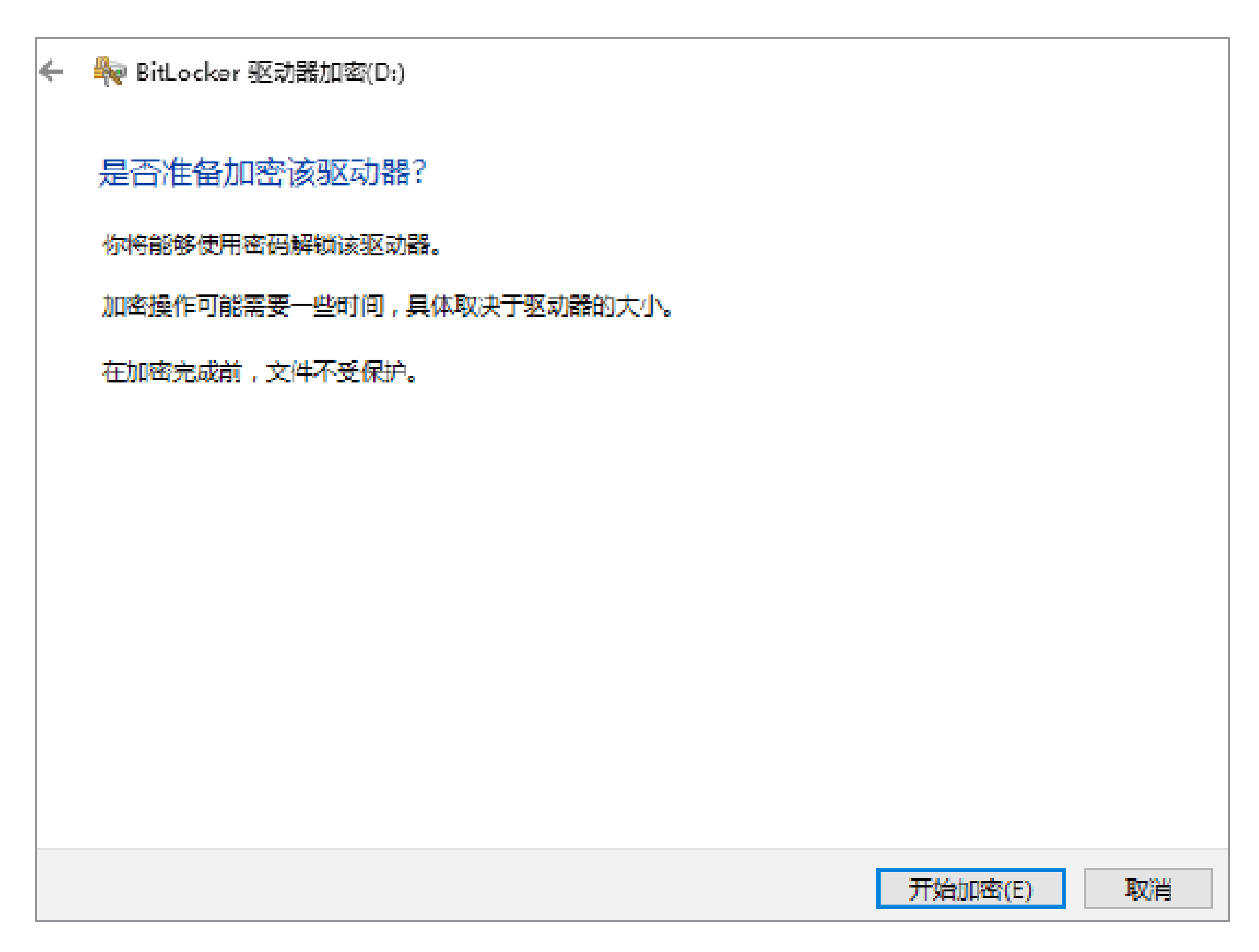
Step 05 单击“下一步”按钮，进入“选择要加密的驱动器空间大小”对话框，如下图所示。



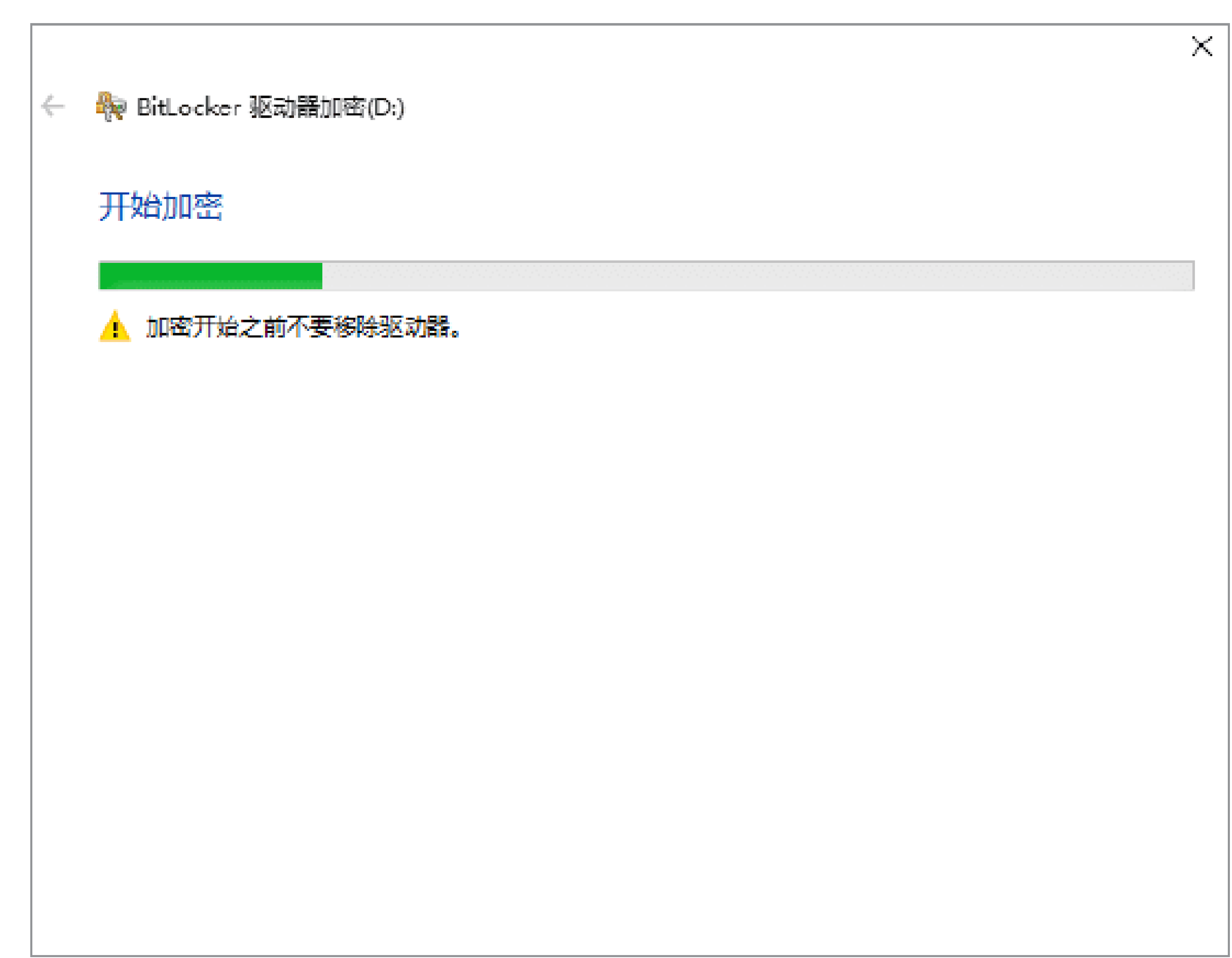
Step 06 单击“下一步”按钮，选择要使用的加密模式，如下图所示。



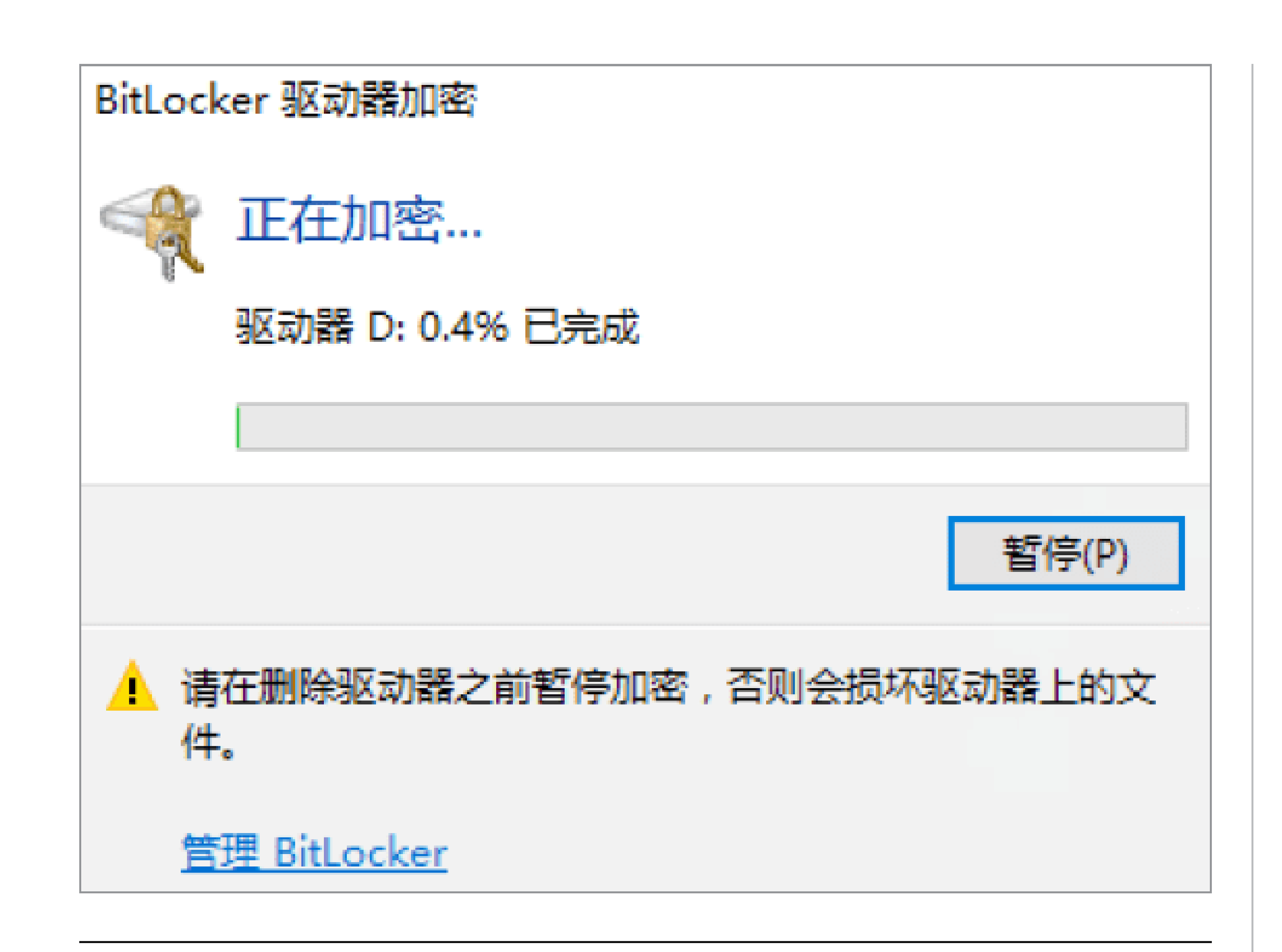
Step 07 单击“下一步”按钮，确认是否准备加密该驱动器，如下图所示。



Step 08 单击“开始加密”按钮，开始对可移动驱动器进行加密，加密的时间与驱动器的容量有关，但是加密过程不能中止，如下图所示。



Step 09 “开始加密”启动完成后，打开“BitLocker驱动器加密”对话框，显示加密的进度，如下图所示。



提示：如果希望加密过程暂停，则单击“暂停”按钮，暂停驱动器的加密，如下图所示。



Step 10 单击“继续”按钮，可继续对驱动器进行加密。加密完成后，将弹出信息提示框，提示用户加密已完成，如下图所示。单击“关闭”按钮，D盘的加密完成。



第8章　浏览器的安全防护

浏览器是进入网页的入口，其功能非常强大，但由于支持JavaScript脚本、ActiveX控件等元素，使得Internet Explorer在浏览网页时留下了许多隐患，因此，保护浏览器的安全也就成了一项刻不容缓的工作。本章介绍浏览器的安全防护，主要内容包括浏览器的攻击方式、自我防护技巧等。

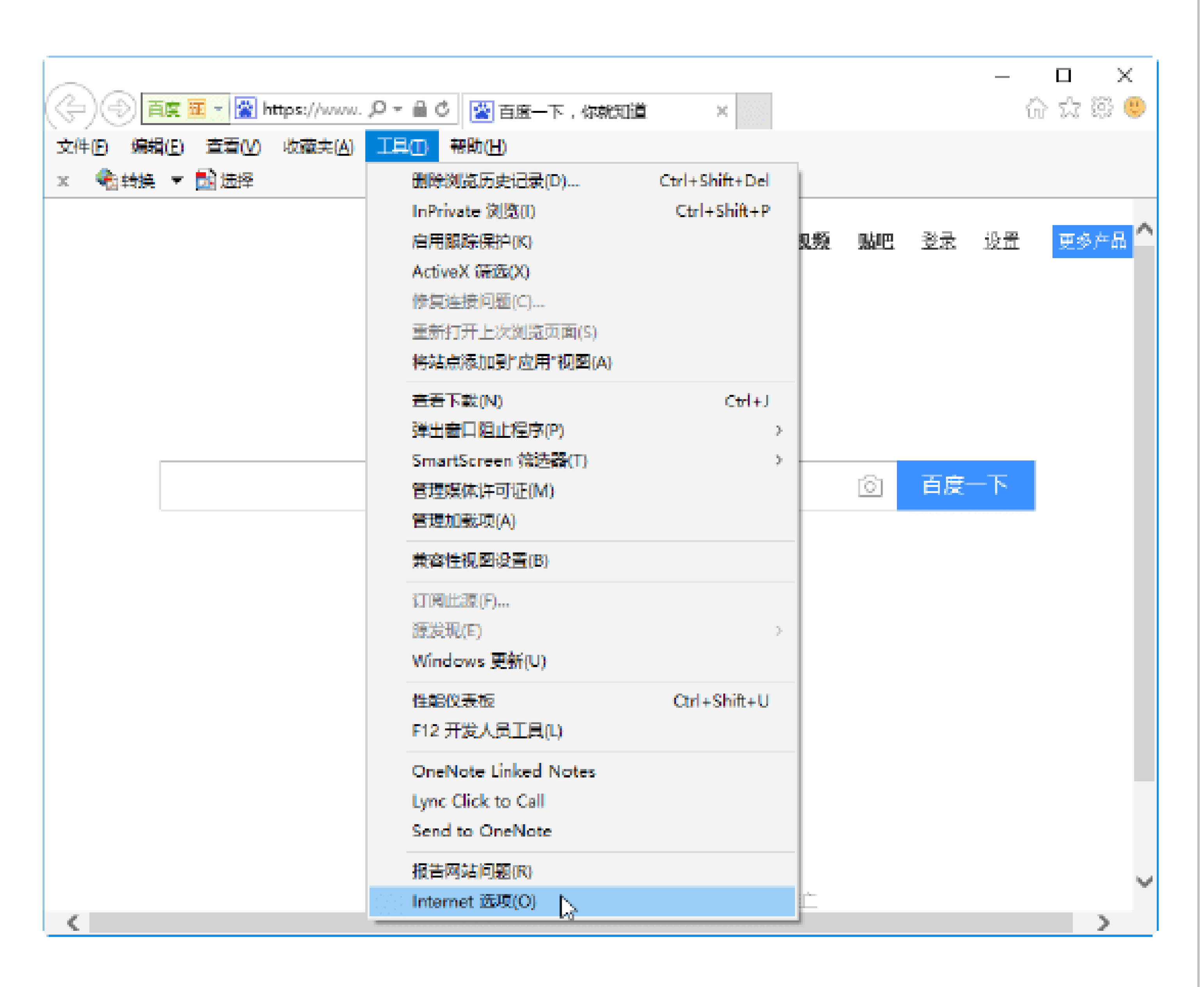
8.1　常见浏览器的攻击方式

浏览器是用户访问网站的主要工具，通过浏览器用户可以访问海量的信息，本节以常用的IE浏览器为例，介绍常见浏览器攻击手法。

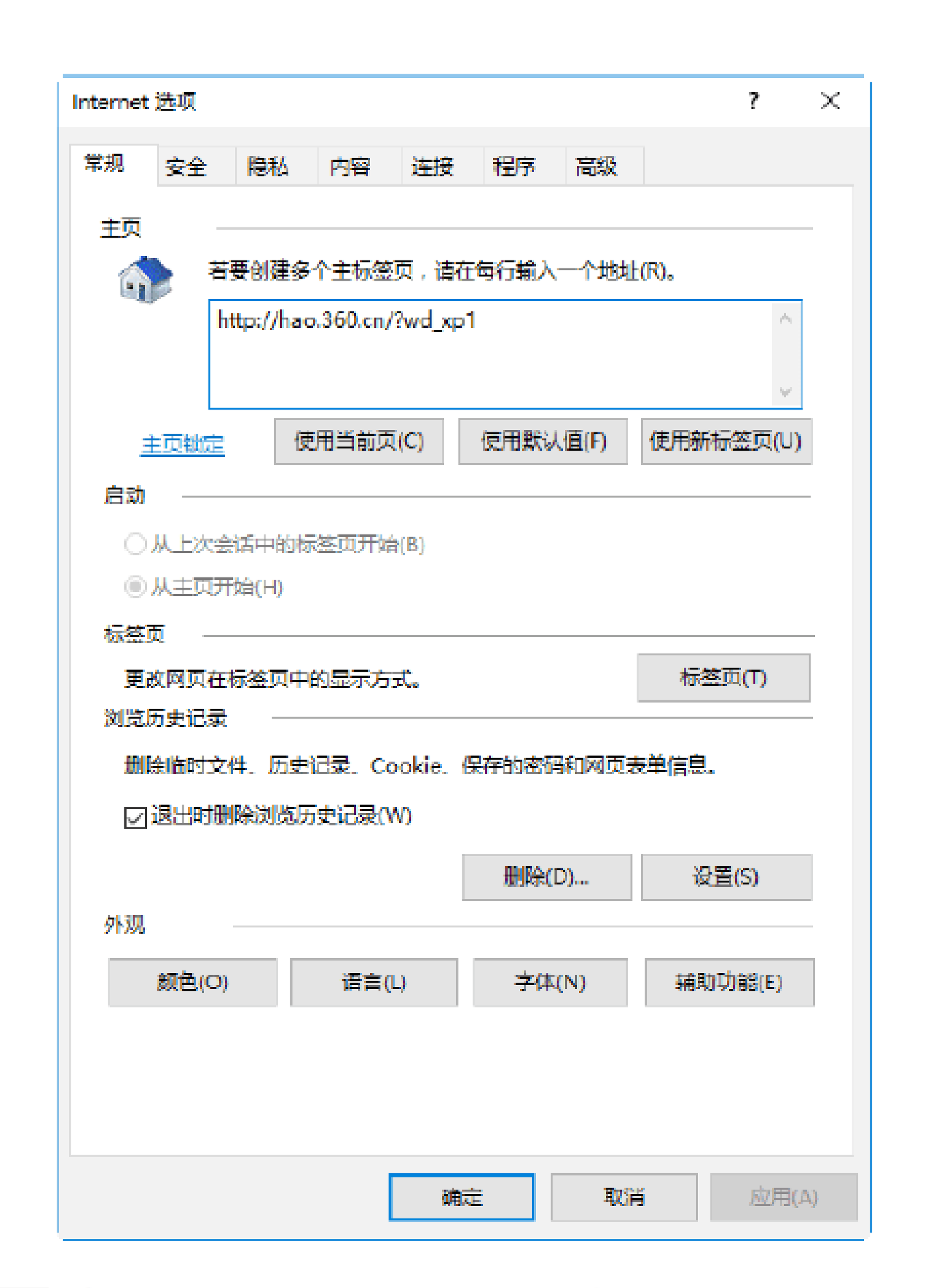
实战1：修改浏览器的默认主页

某些网站为了提高自己的访问量和进行广告宣传，使用恶意代码将用户设置的主页修改为自己的网页。解决这一问题最简单的方式是设置“Internet选项”对话框。具体的操作步骤如下。

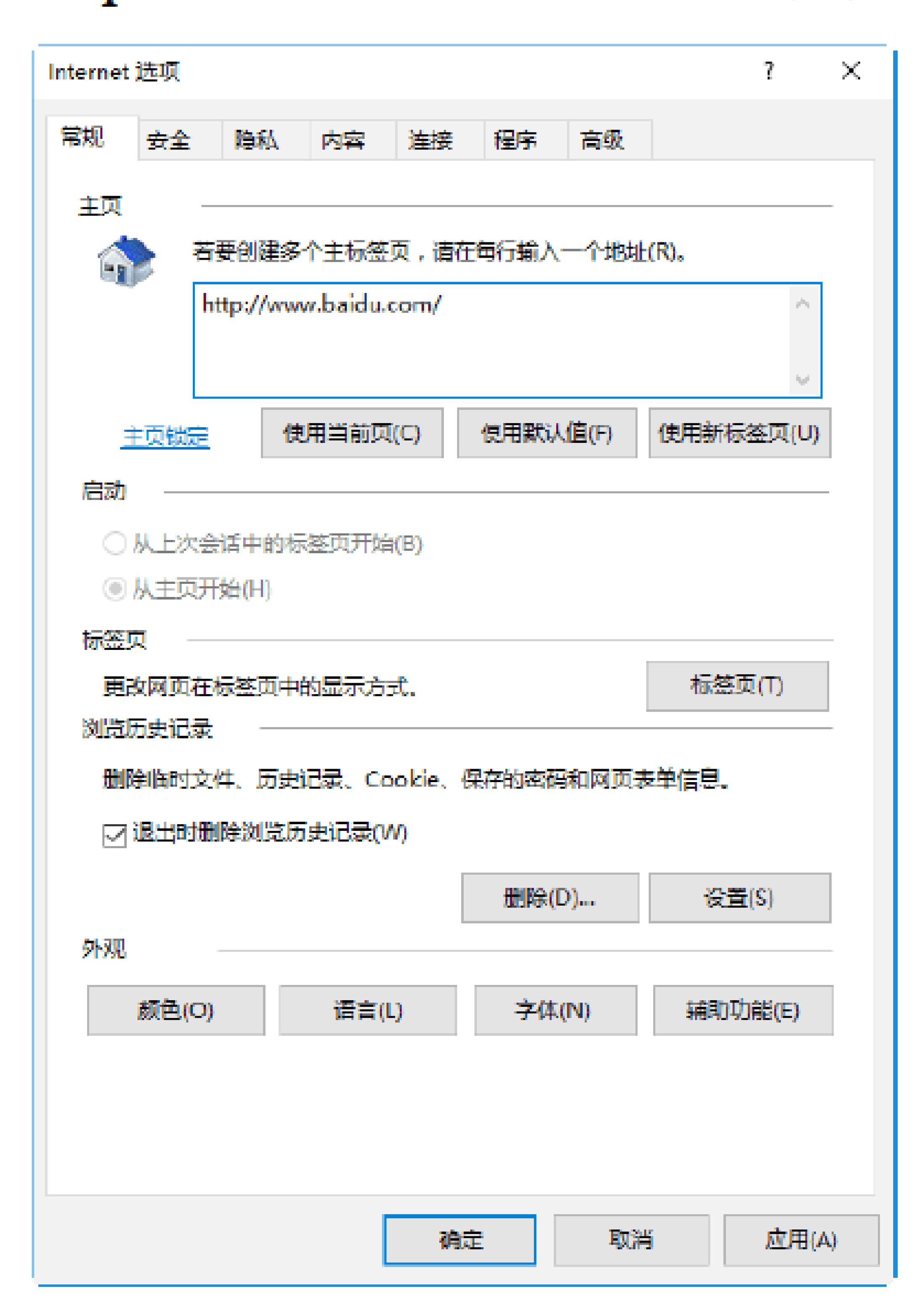
Step 01 打开IE浏览器，在其中选择“工具”→“Internet选项”选项，如下图所示。



Step 02 打开“Internet选项”对话框，在其中选择“常规”选项卡，如下图所示。



Step 03 在“主页”设置区域中的“地址”文本框中输入自己需要的主页，如这里输入百度的网址http://www.baidu.com/，如下图所示。



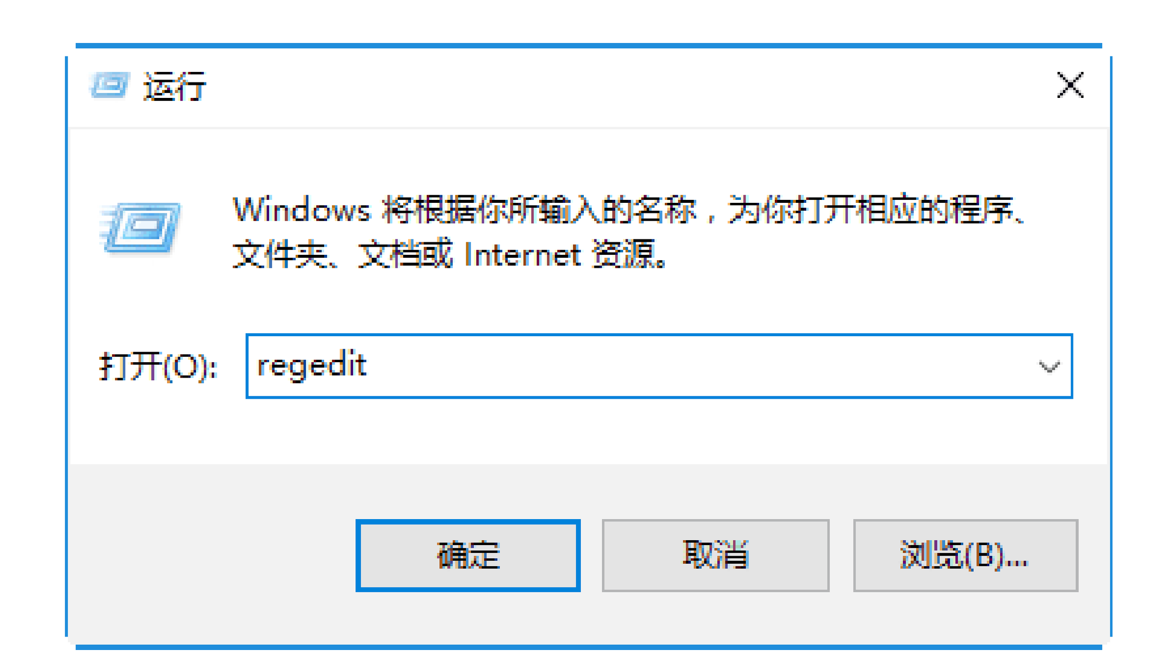
Step 04 单击“确定”按钮，这样就可以把主页设置为百度。双击桌面上的“IE浏览器”图标，打开IE浏览器主页，即百度首页，如下图所示。



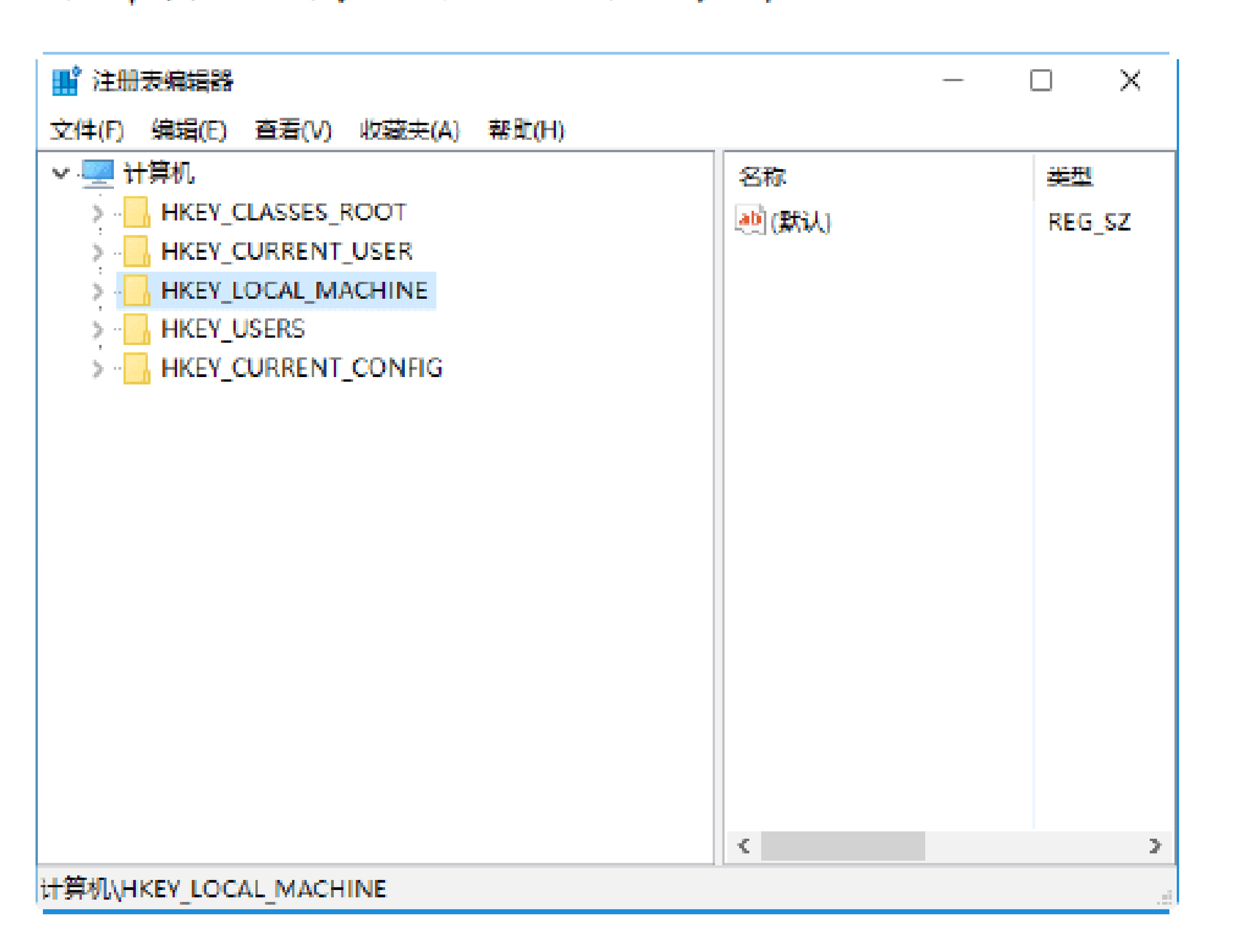
实战2：恶意更改浏览器标题栏

网页浏览器的标题栏也是黑客攻击浏览器常用的方法之一，具体表现为浏览器的标题栏被加入一些固定不变的广告等信息。针对这种攻击手法，用户可以通过修改注册表清除标题栏中的广告等信息。具体的操作步骤如下。

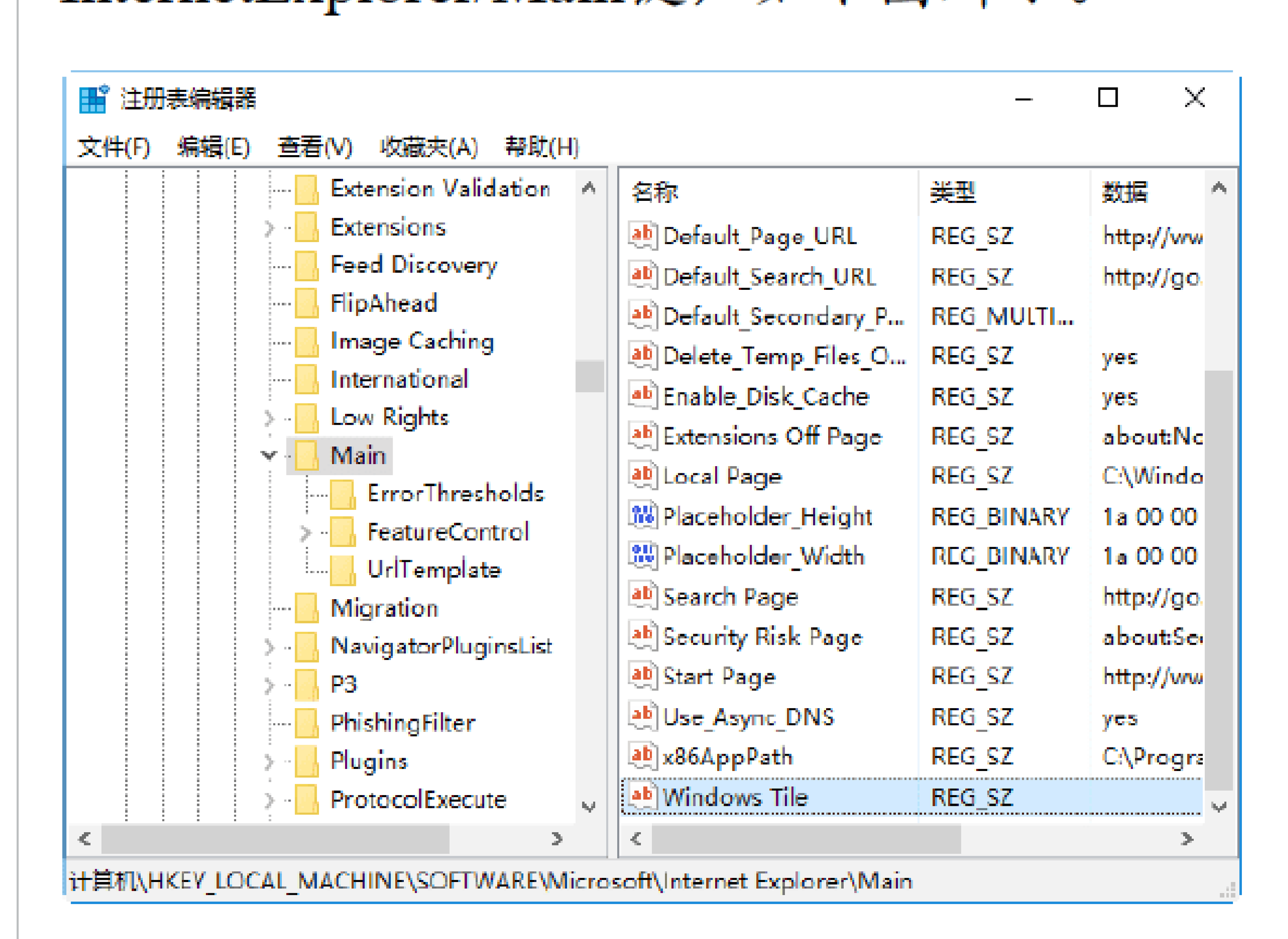
Step 01 打开“运行”对话框，在“打开”文本框中输入regedit命令，如下图所示。



Step 02 单击“确定”按钮，即可打开“注册表编辑器”窗口，如下图所示。

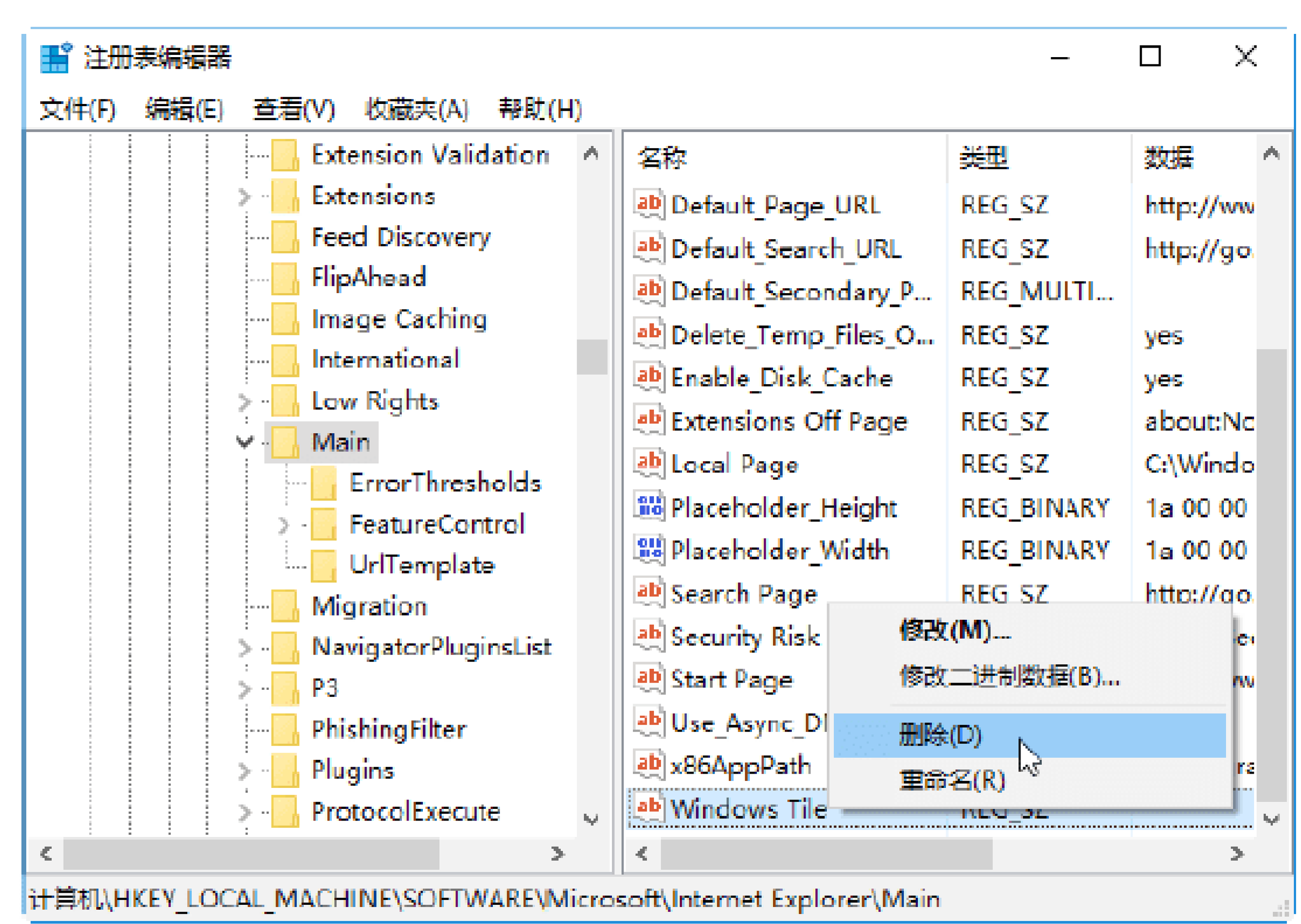


Step 03 在左侧窗格中选择HKEY_LOCAL_MACHINE\Software\Microsoft\InternetExplorer/Main键，如下图所示。

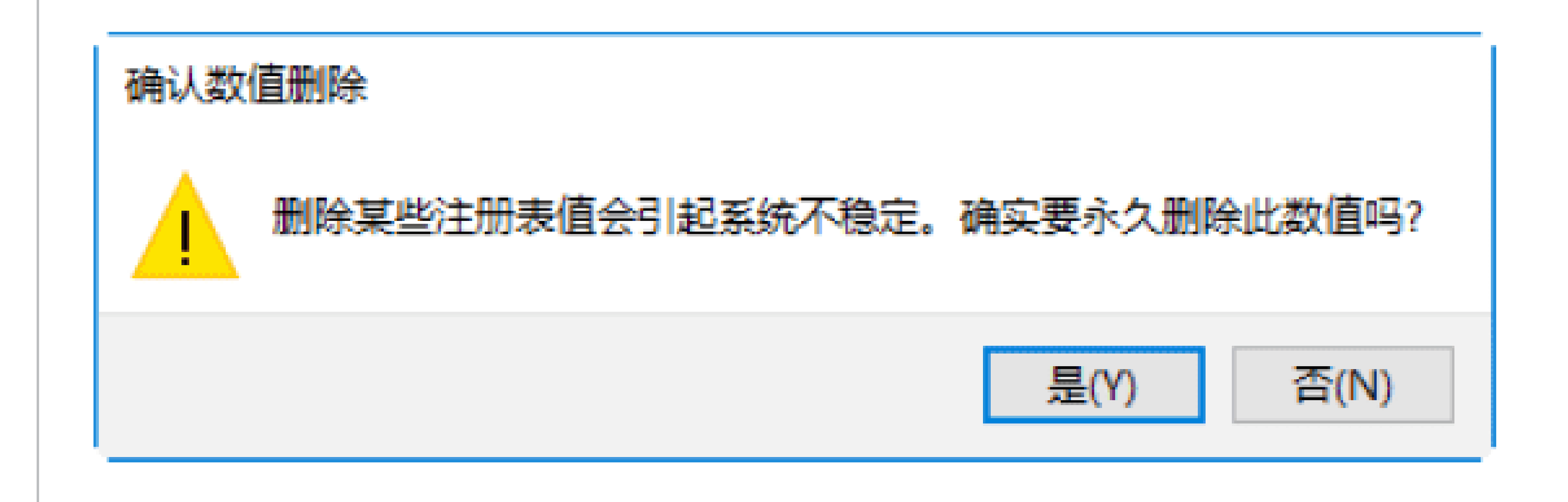


Step 04 在右侧窗格中选中Windows Tile键值项并右击，在弹出的快捷菜单中选择“删除”选项，如下图所示。





Step 05 打开“确认数值删除”对话框，提示用户“确实要永久删除此数值吗？”，如下图所示。



Step 06 单击“是”按钮，即可完成数值删除操作，关闭注册表编辑器，然后重新启动计算机，当再次使用IE浏览器浏览网页时，就会发现标题栏中的广告等信息已经被删除了，如下图所示。



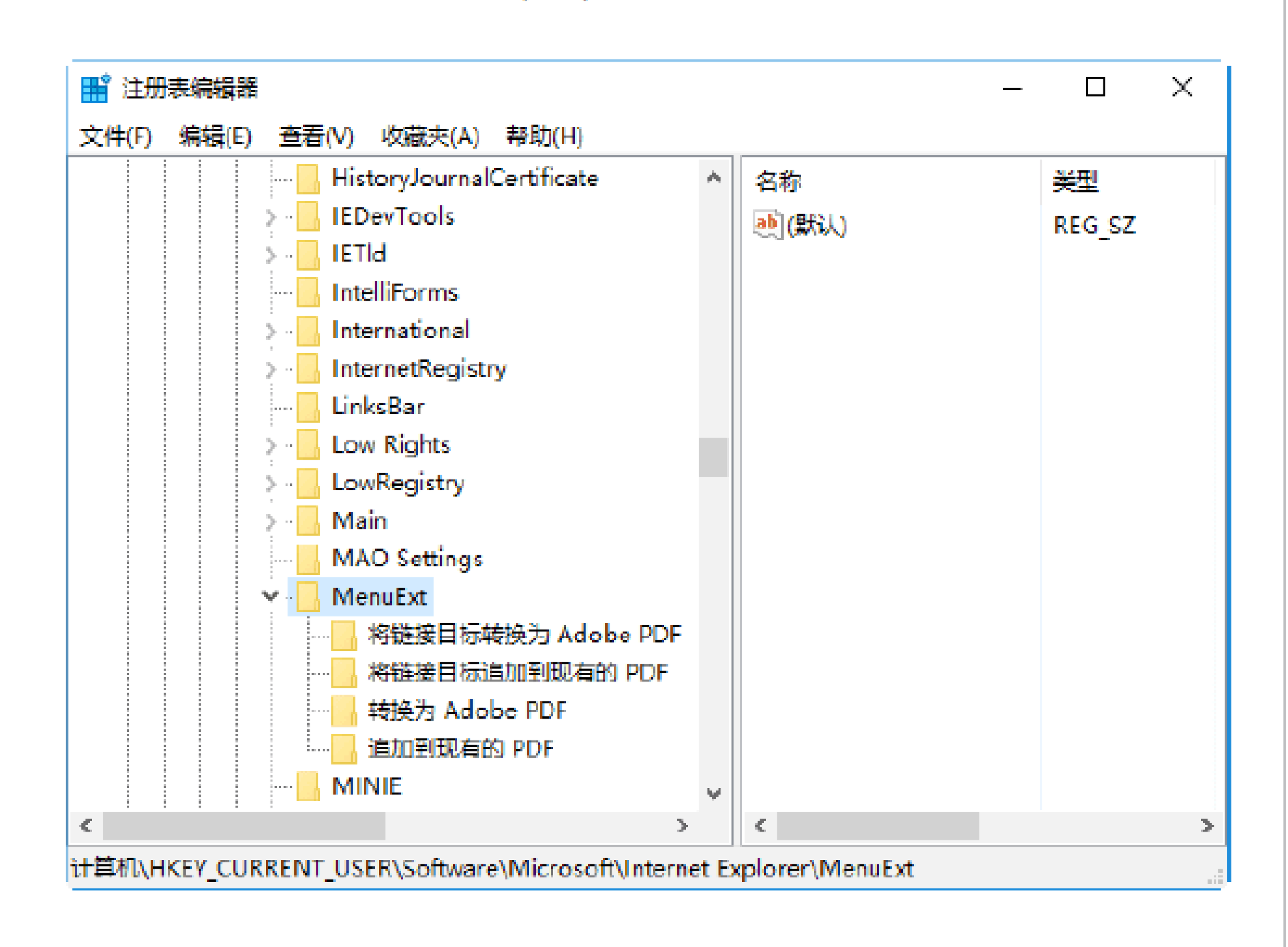
实战3：强行修改浏览器的右键菜单

被强行修改右键菜单的现象主要表现在以下两方面。

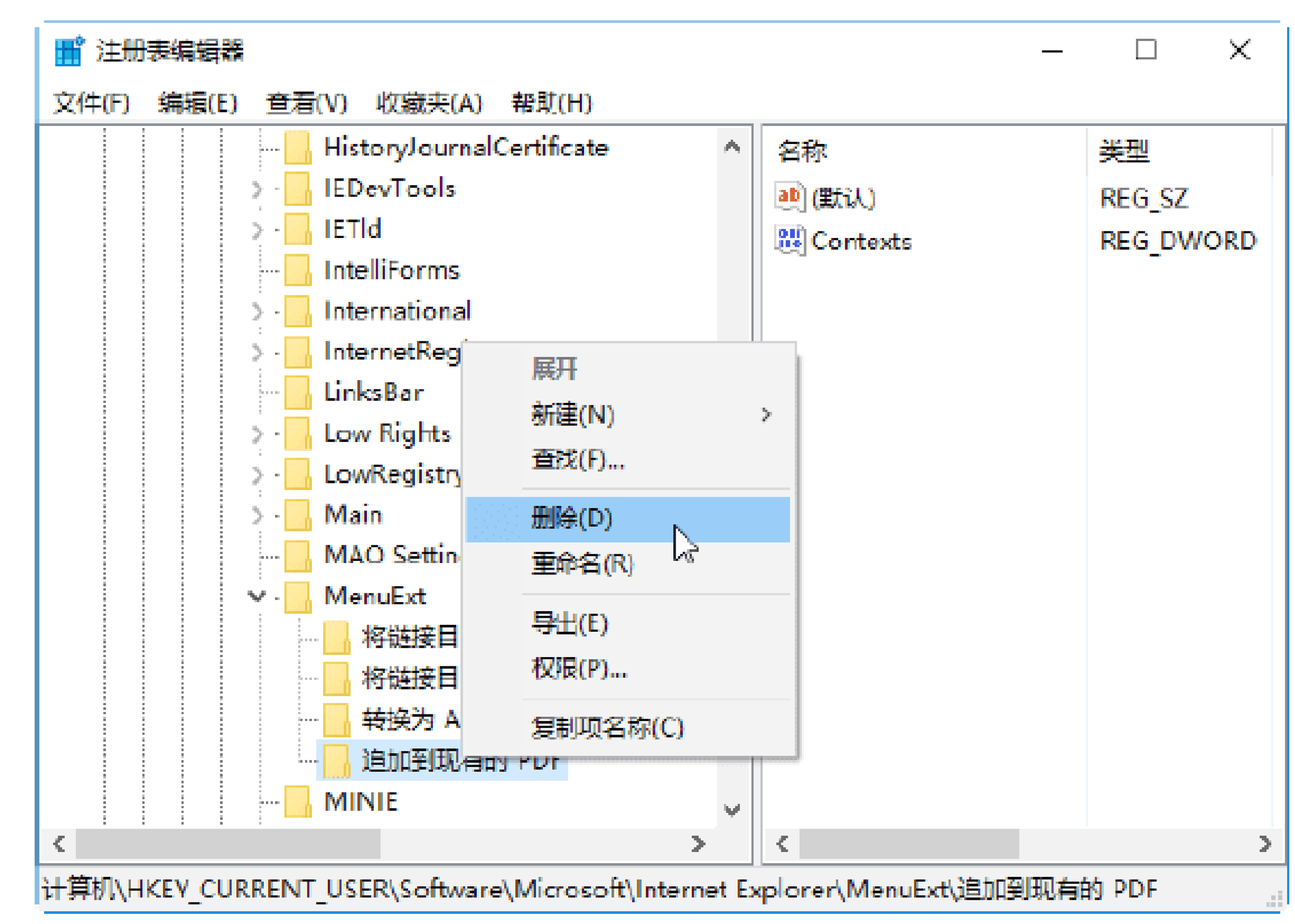
- 右键快捷菜单被添加非法网站链接。
- 右键弹出快捷菜单功能被禁用失常，在IE浏览器中单击鼠标右键无反应。

针对浏览器右键菜单中出现的非法链接这种情况，修复的具体操作步骤如下。

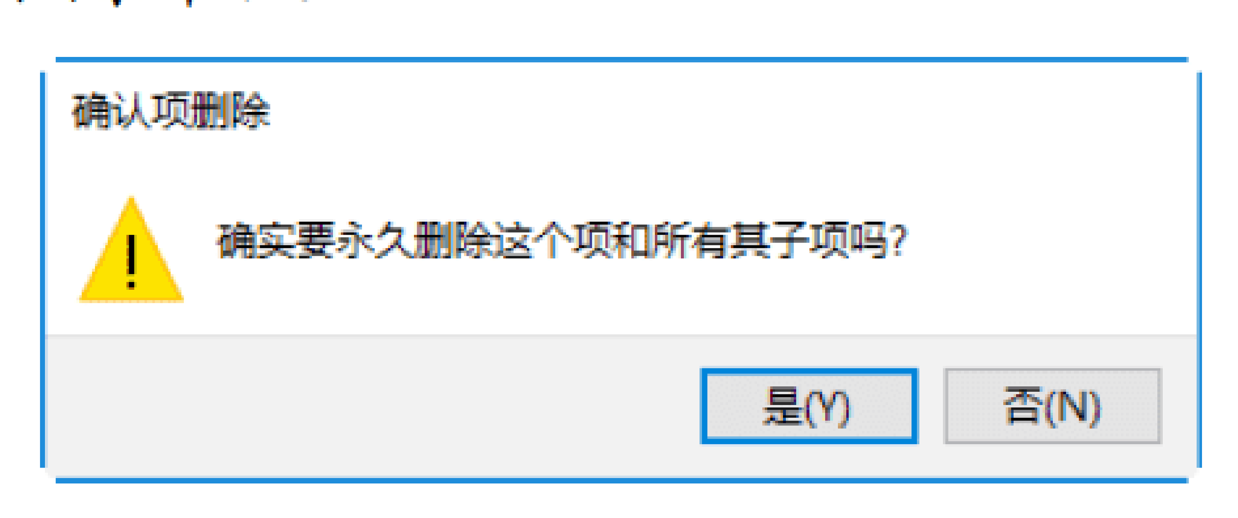
Step 01 打开“注册表编辑器”窗口，在左侧窗格中单击展开HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt，如下图所示。



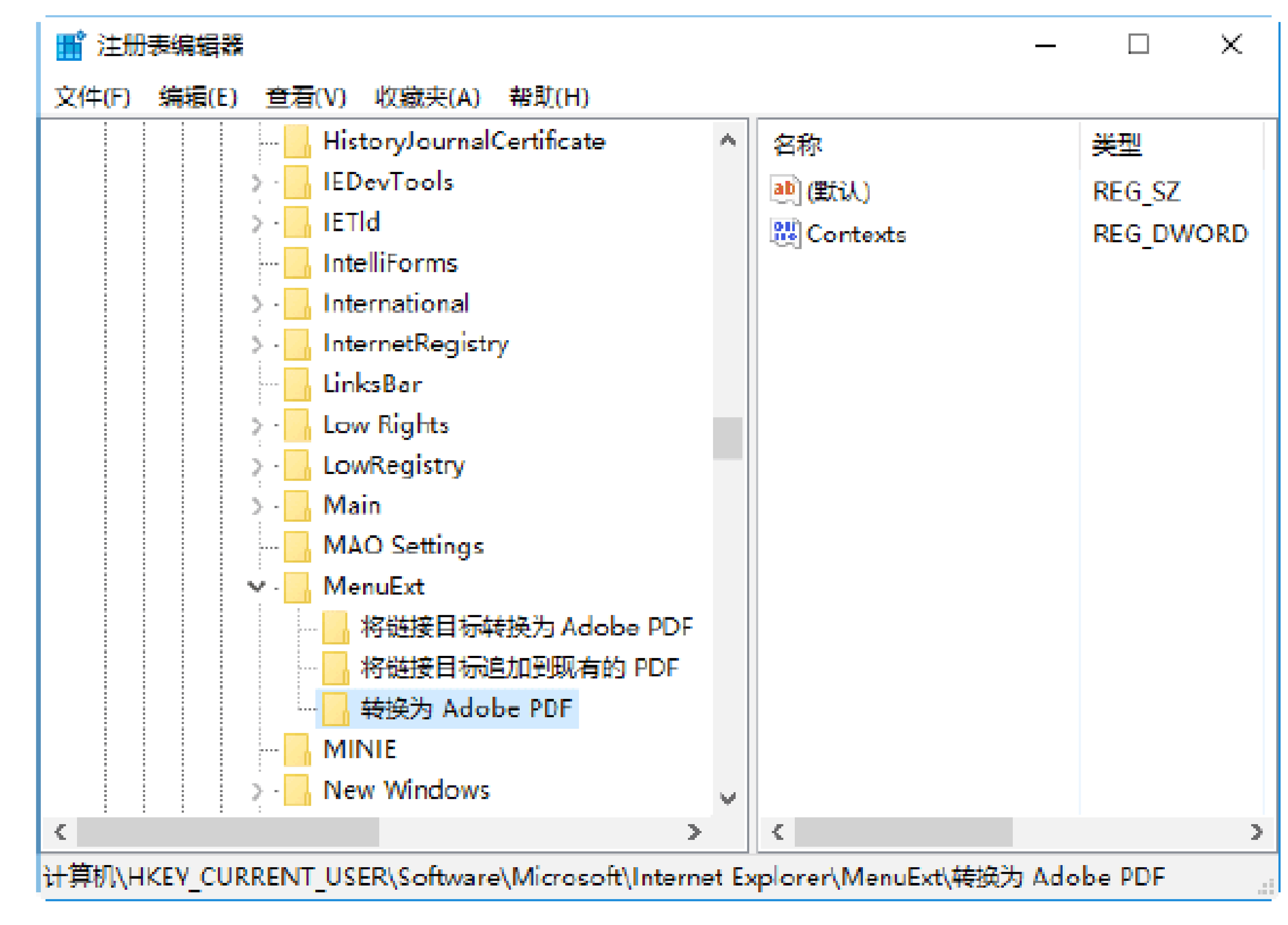
Step 02 IE的右键菜单都在这里设置，在其中选择非法的右键链接，如这里选择“追加到现有的PDF”选项并右击，在弹出的快捷菜单中选择“删除”选项，如下图所示。



Step 03 打开“确认项删除”对话框，提示用户是否确实要删除这个项和所有其子项，如下图所示。



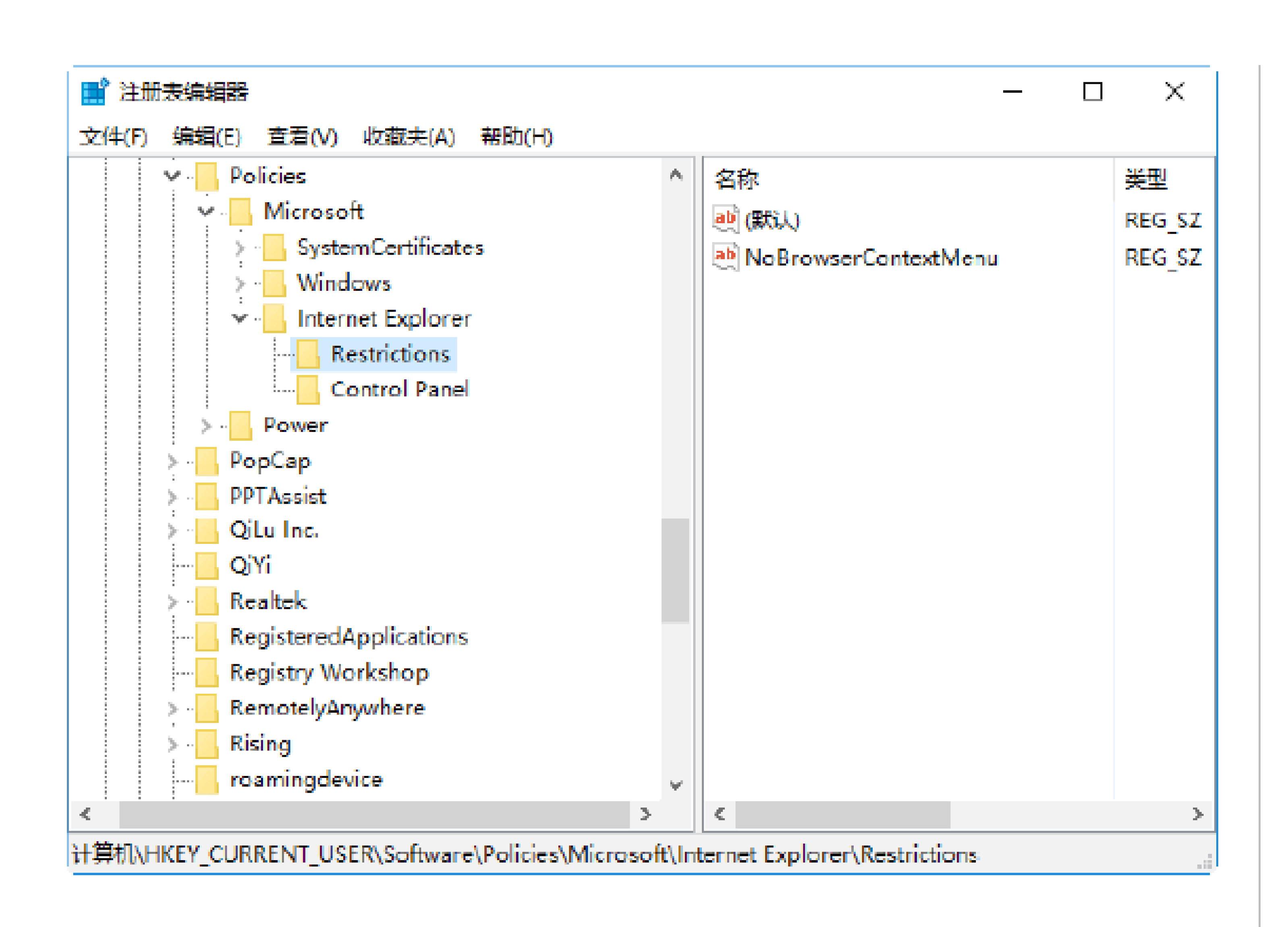
Step 04 单击“是”按钮，即可将该项删除，如下图所示。



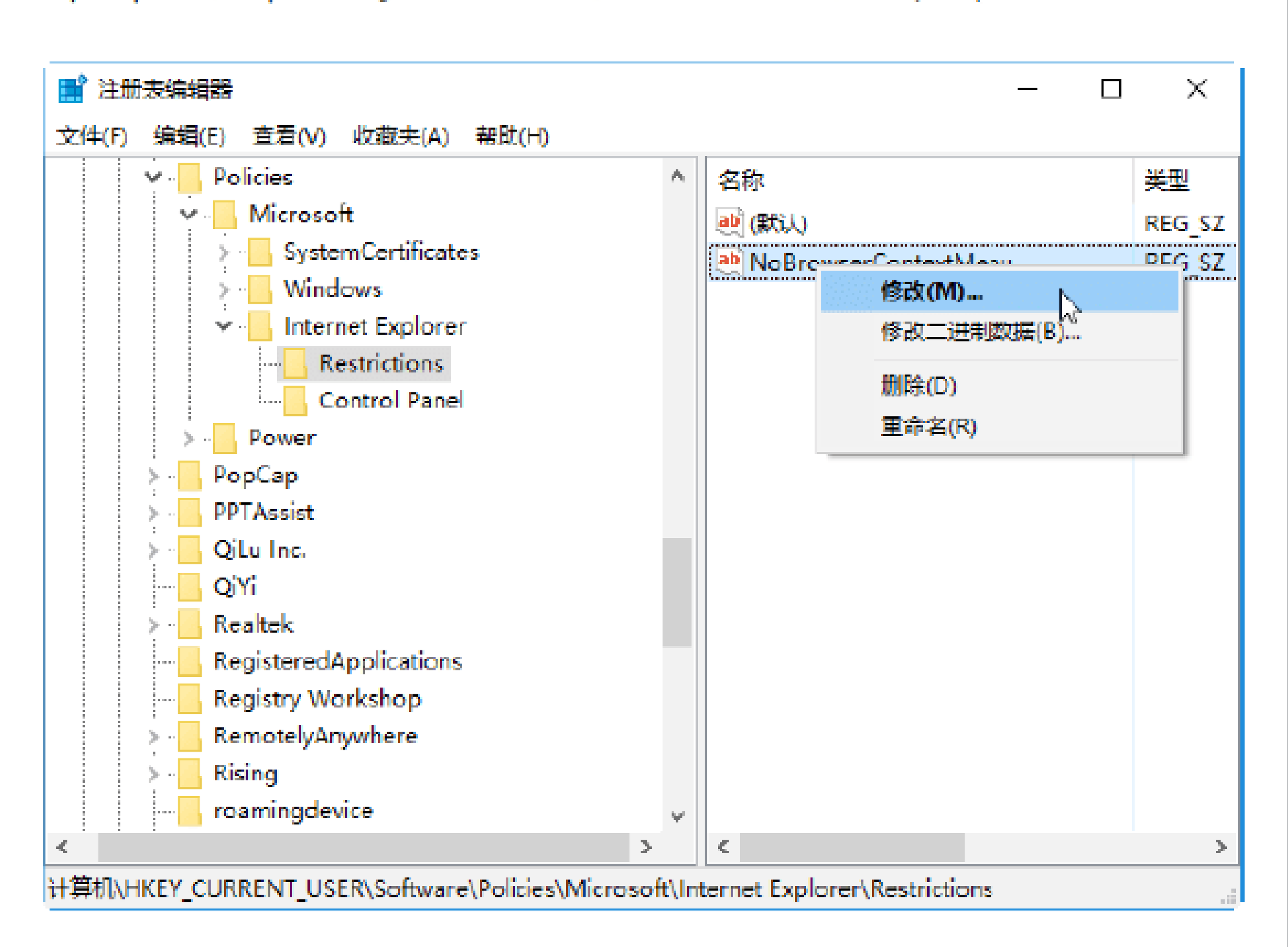
提示：在删除前，最好先展开MenuExt主键检查一下，里面是否会有一个子键，其内容是指向一个HTML文件的，找到这个文件路径，然后根据此路径将该文件也删除，这样才能彻底清除。

针对右键菜单打不开的情况，修复的操作步骤如下。

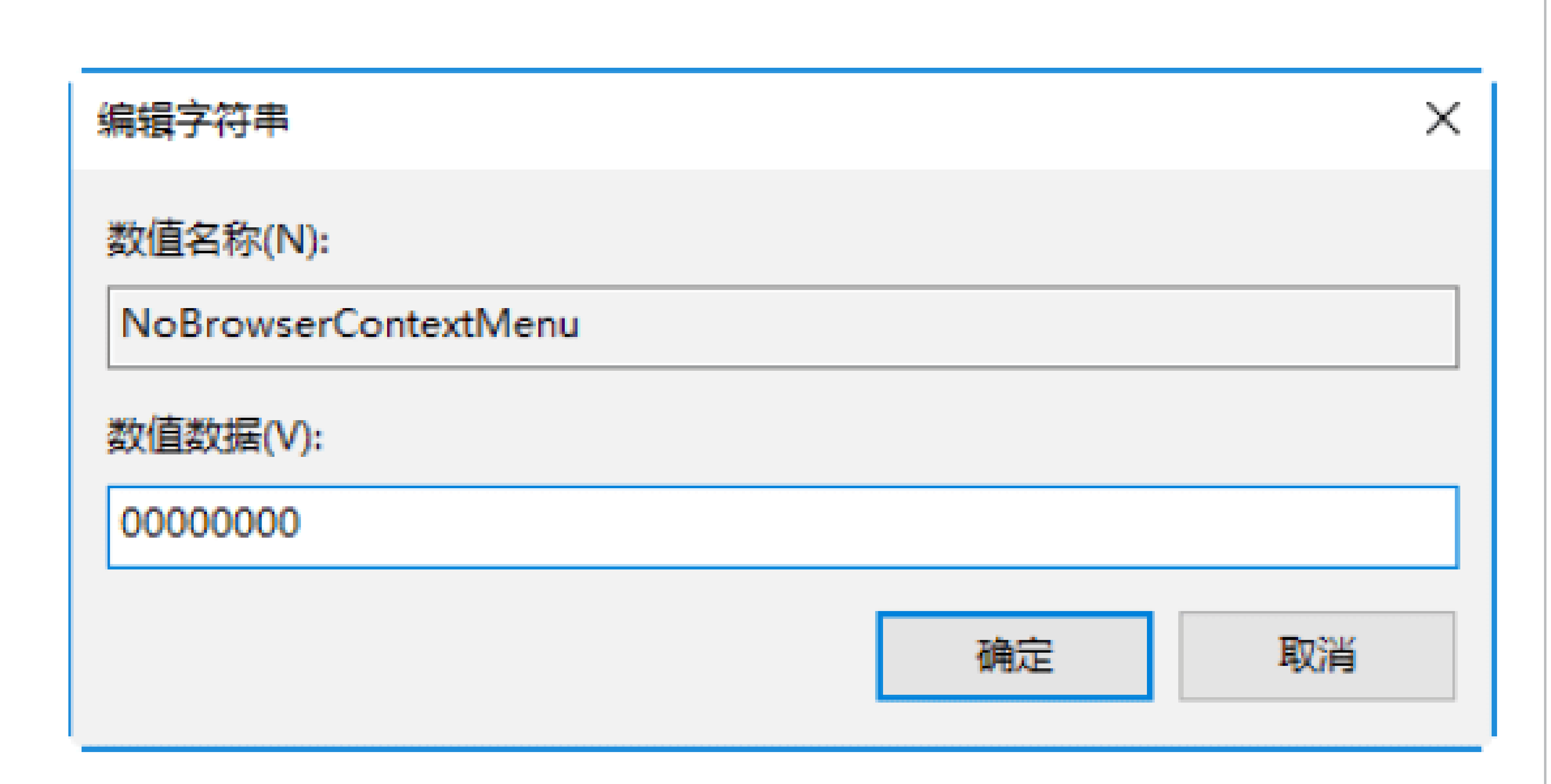
Step 05 打开“注册表编辑器”窗口，在左侧窗格中单击展开HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions，如下图所示。



Step 06 在右侧窗格中选中NoBrowserContextMenu键值并右击，在弹出的快捷菜单中选择“修改”选项，如下图所示。

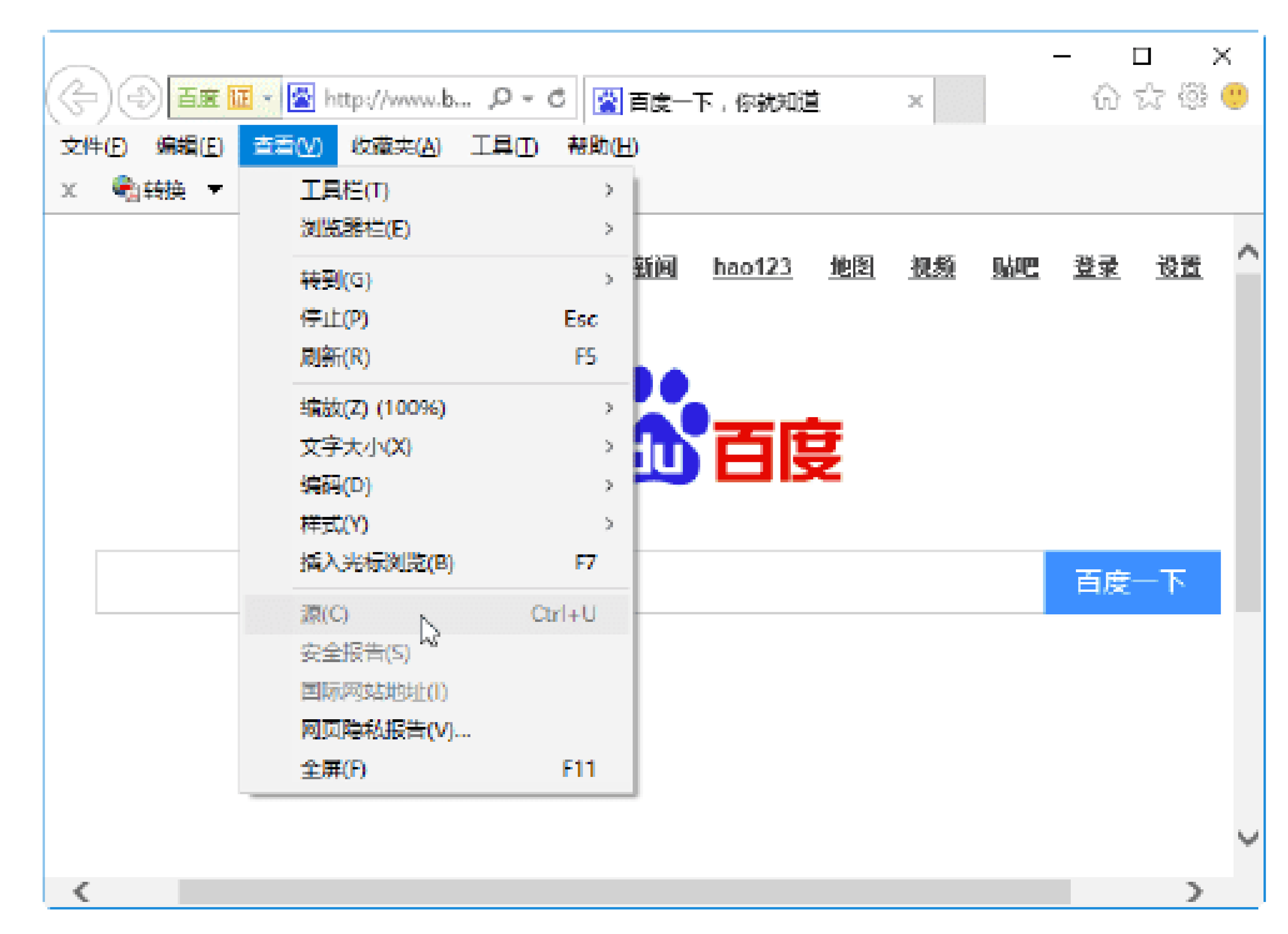


Step 07 打开“编辑字符串”对话框，在“数值数据”文本框中输入00000000。单击“确定”按钮，即可完成IE浏览器的修复，如下图所示。

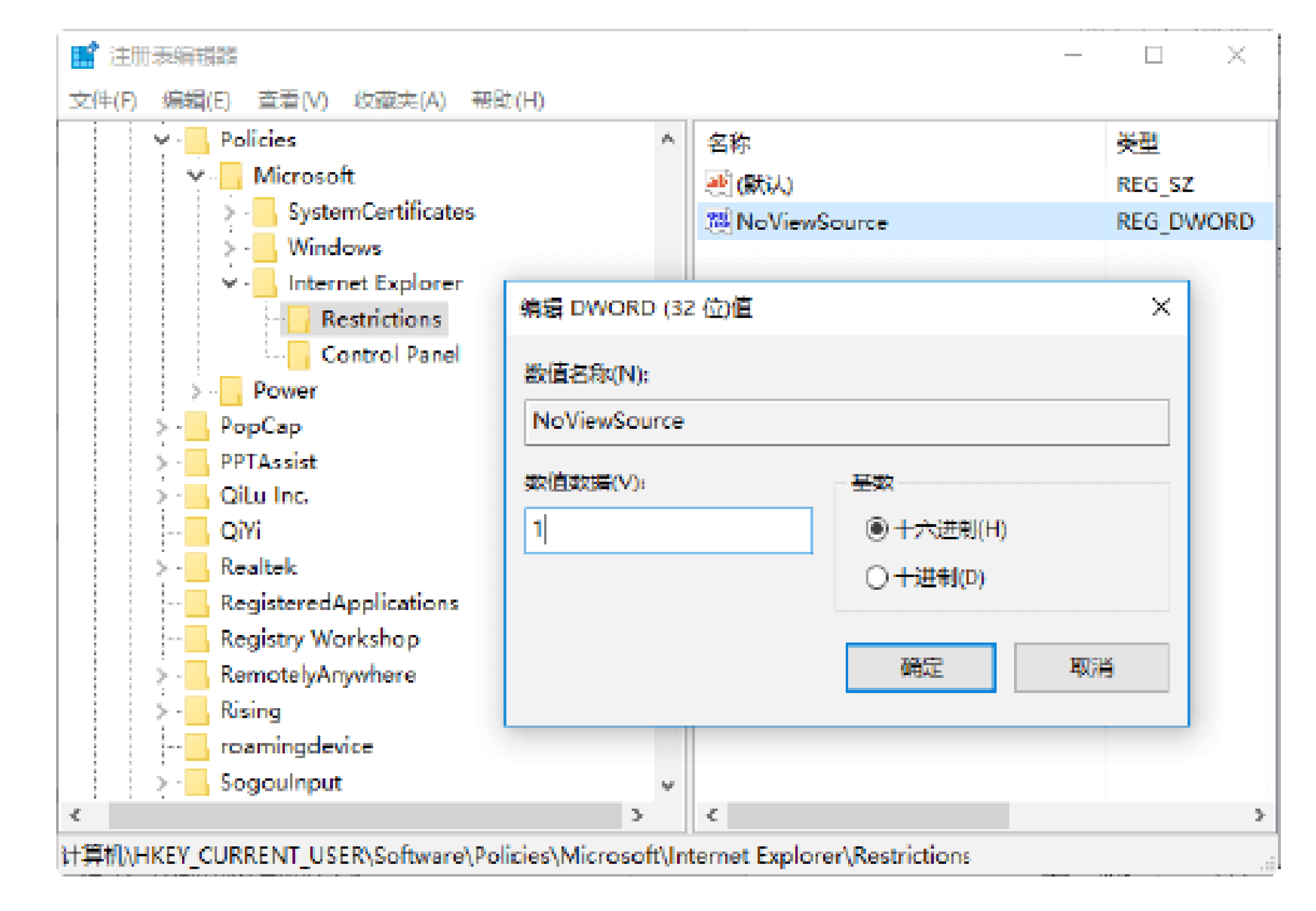


实战4：禁用浏览器的“源”菜单命令

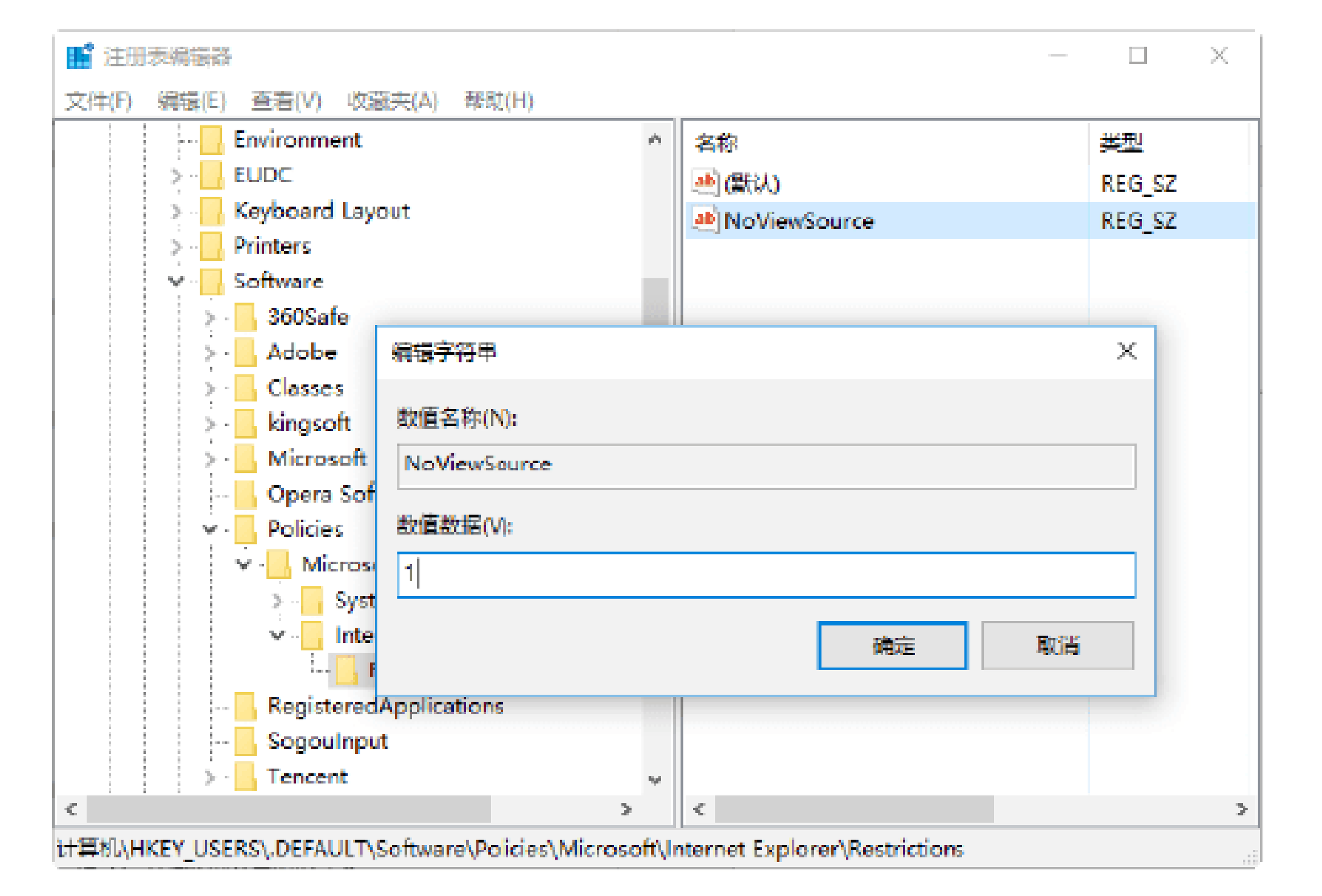
一般网页浏览器都为用户提供查看网页源文件的菜单命令，即“源”菜单命令，该菜单常常受到黑客的攻击，具体表现为被禁用，如下图所示。



出现这种现象的原因是恶意代码修改了注册表的键值，具体位置在HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer下建立子键Restrictions。然后在Restrictions下面建立一个DWORD值，名称为NoViewSource，值为1，如下图所示。



另外，在HKEY_USERS\.DEFAULT\Software\Policies\Microsoft\Internet Explorer\Restrictions下，将DWORD值NoViewSource的键值改为1，如下图所示。

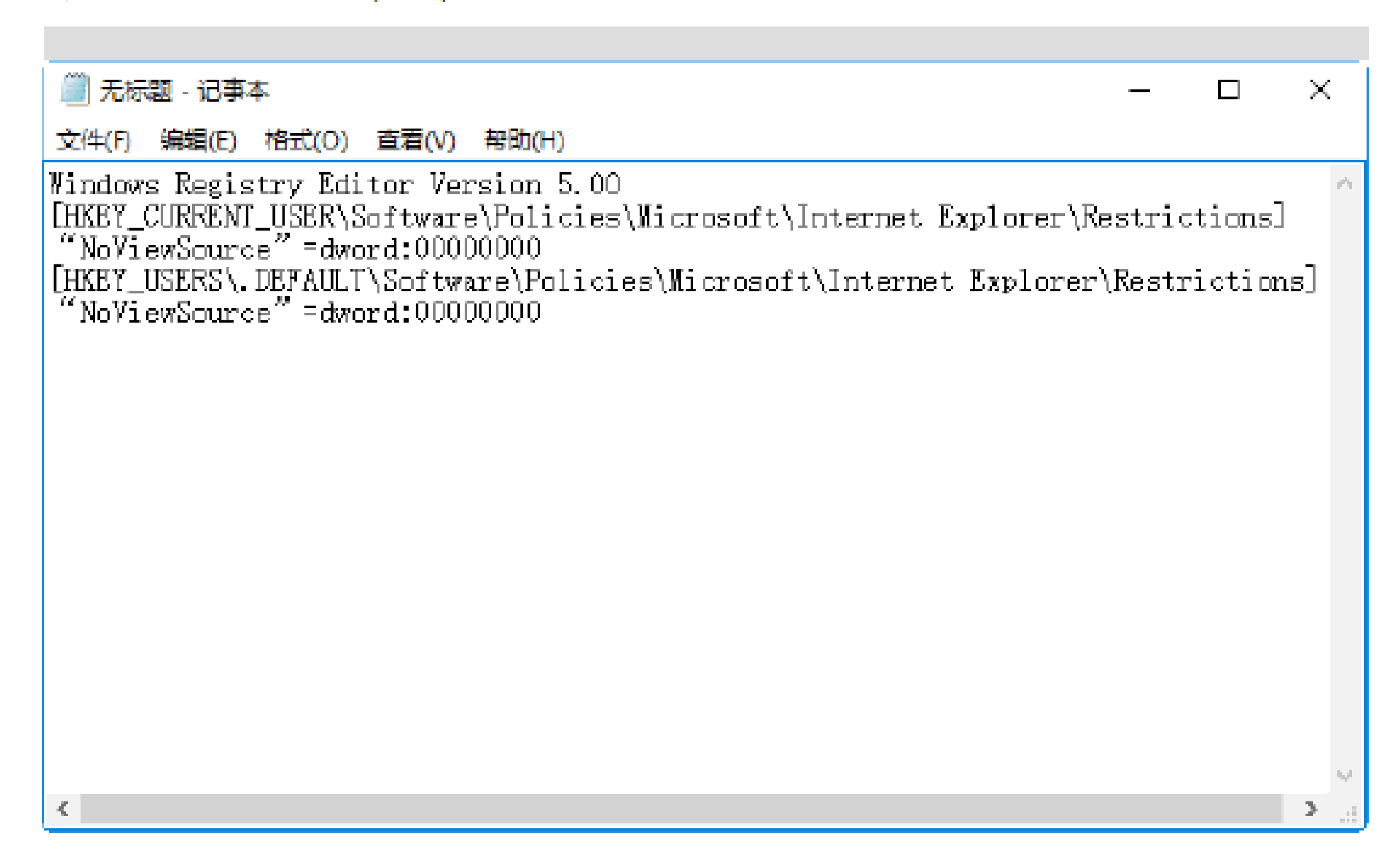




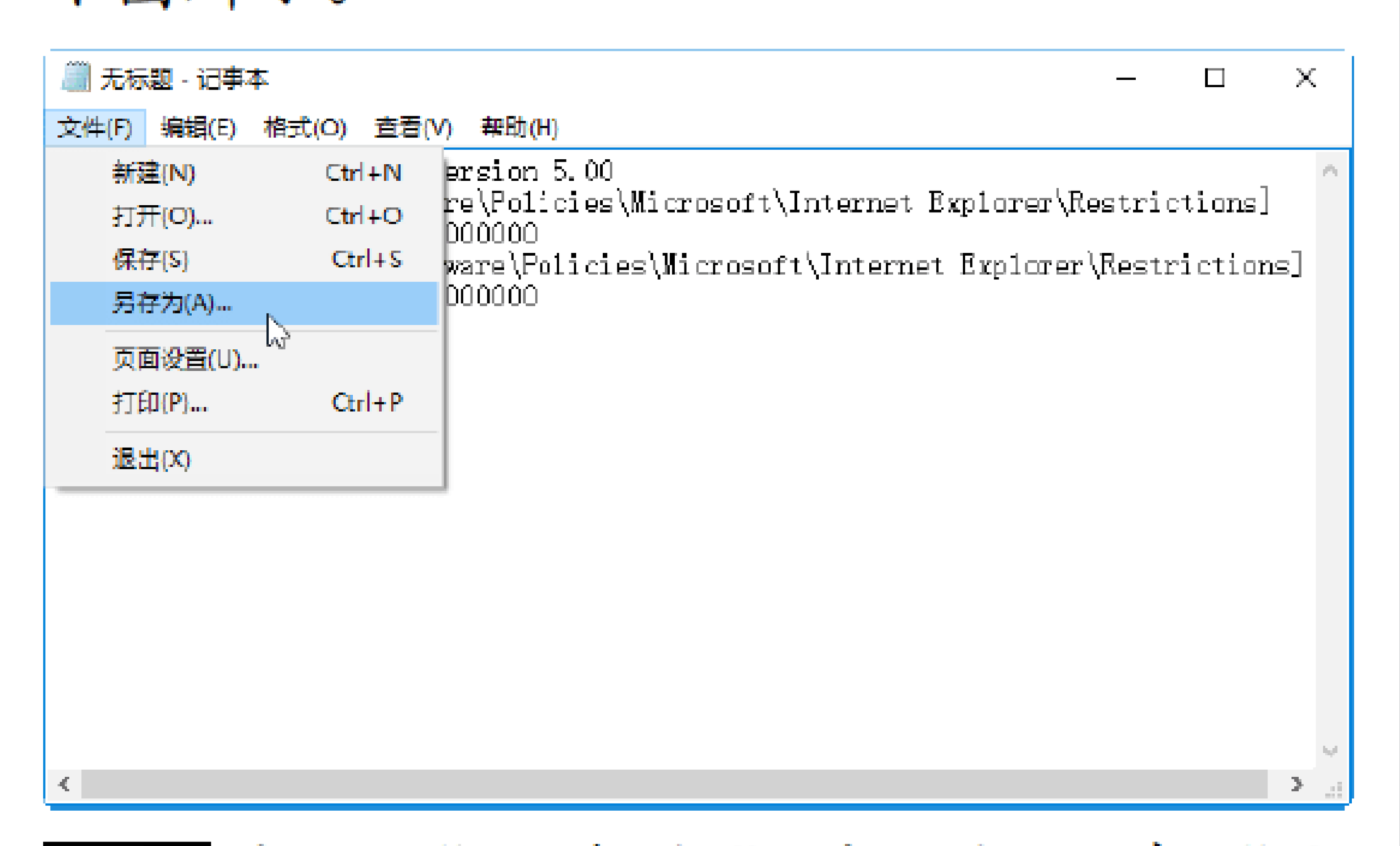
通过上面这些键值的修改，就可以达到使“查看”菜单下中的“源文件”被禁用的目的。

在明白了问题的所在之后，下面就可以通过以下方法进行修复。

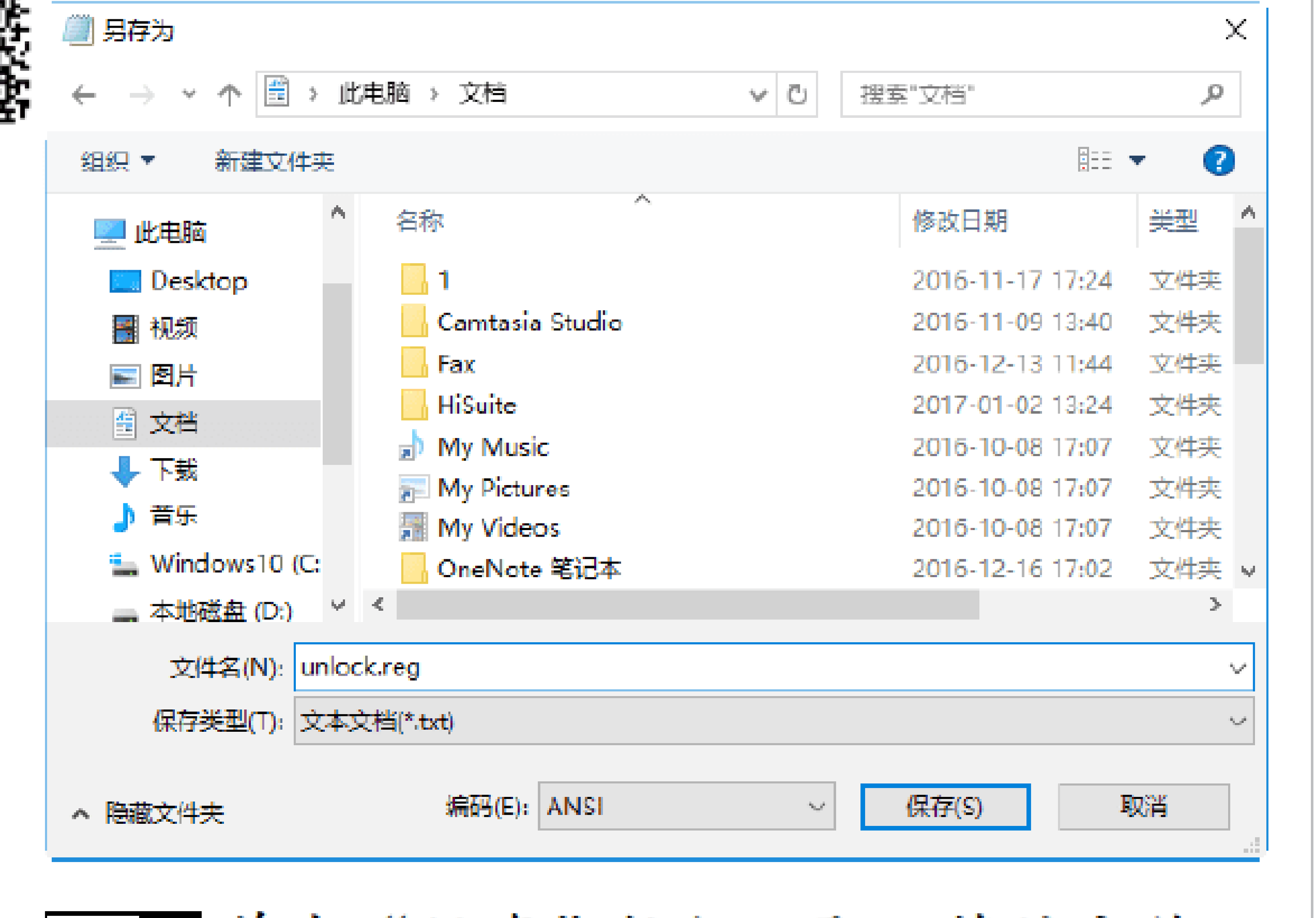
Step 01 打开记事本文件，在其中输入以下内容，如下图所示。



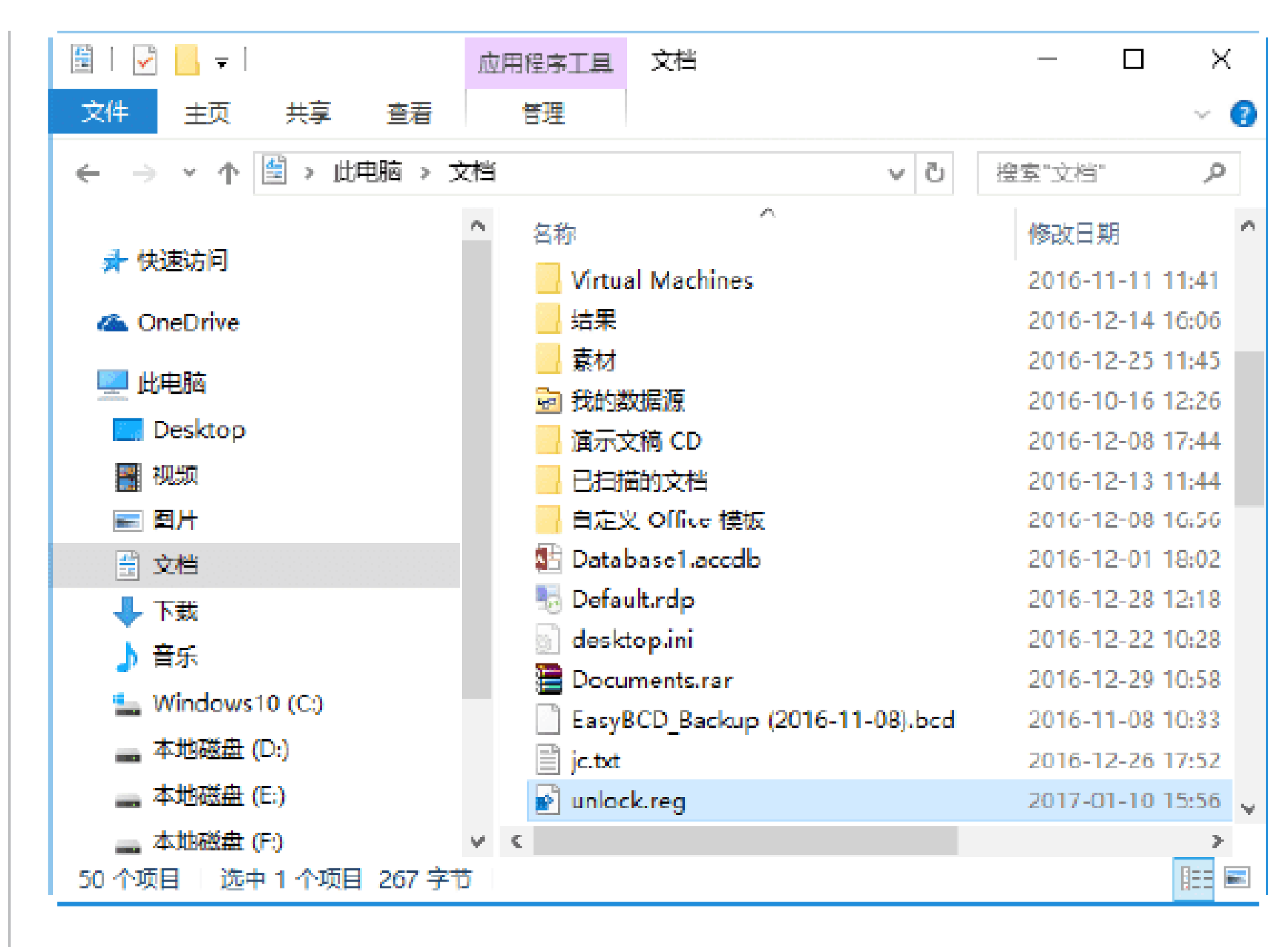
Step 02 选择"文件"→"另存为"选项，如下图所示。



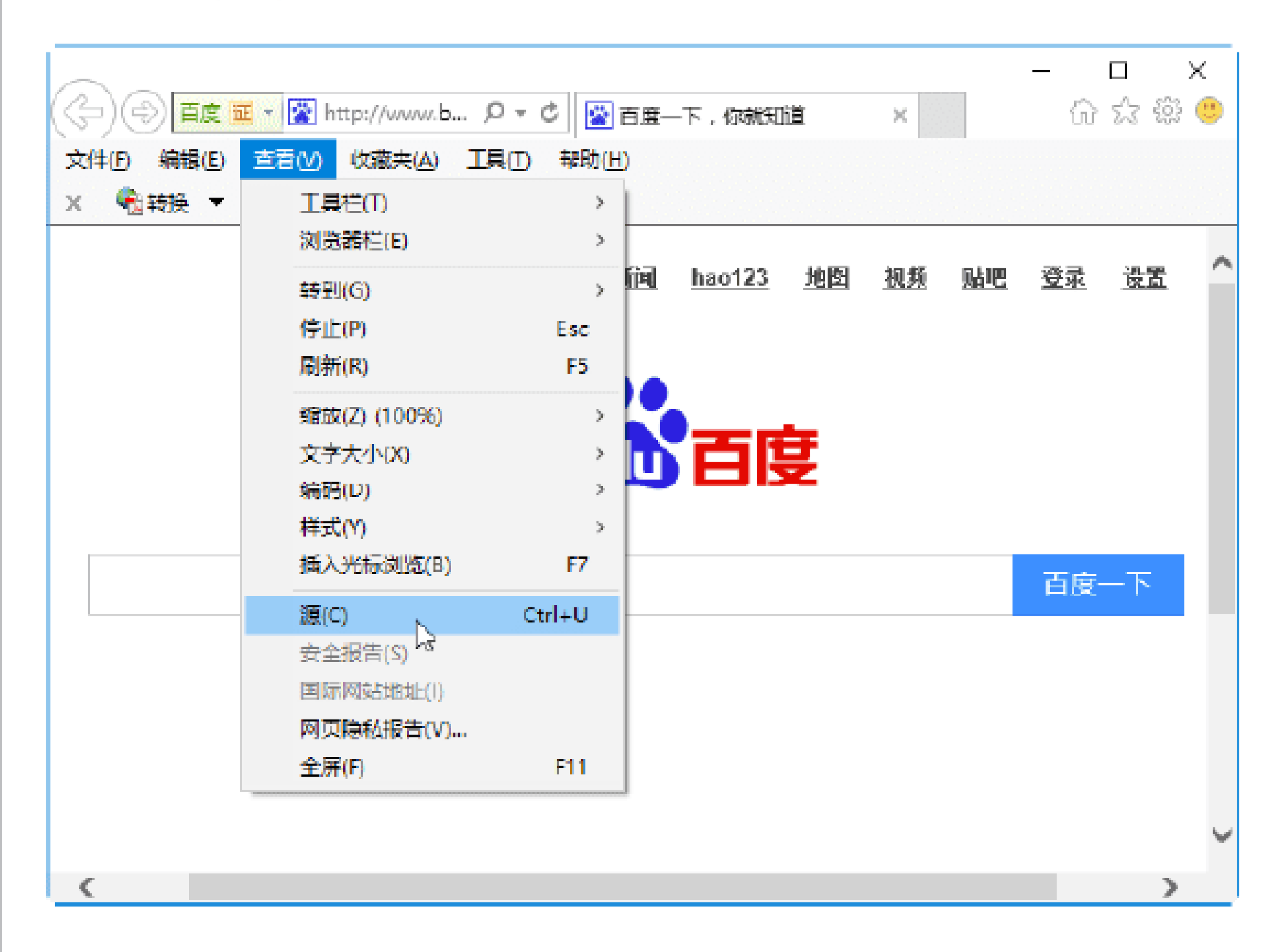
Step 03 打开"另存为"对话框，在"文件名"文本框中输入文件名，这里输入unlock.reg，如下图所示。



Step 04 单击"保存"按钮，即可将该文件以注册表的形式保存，如下图所示。



Step 05 将该文件导入到注册表中，无须重新启动计算机，这时重新运行IE浏览器，就会发现IE的"源"菜单项即可恢复使用，如下图所示。

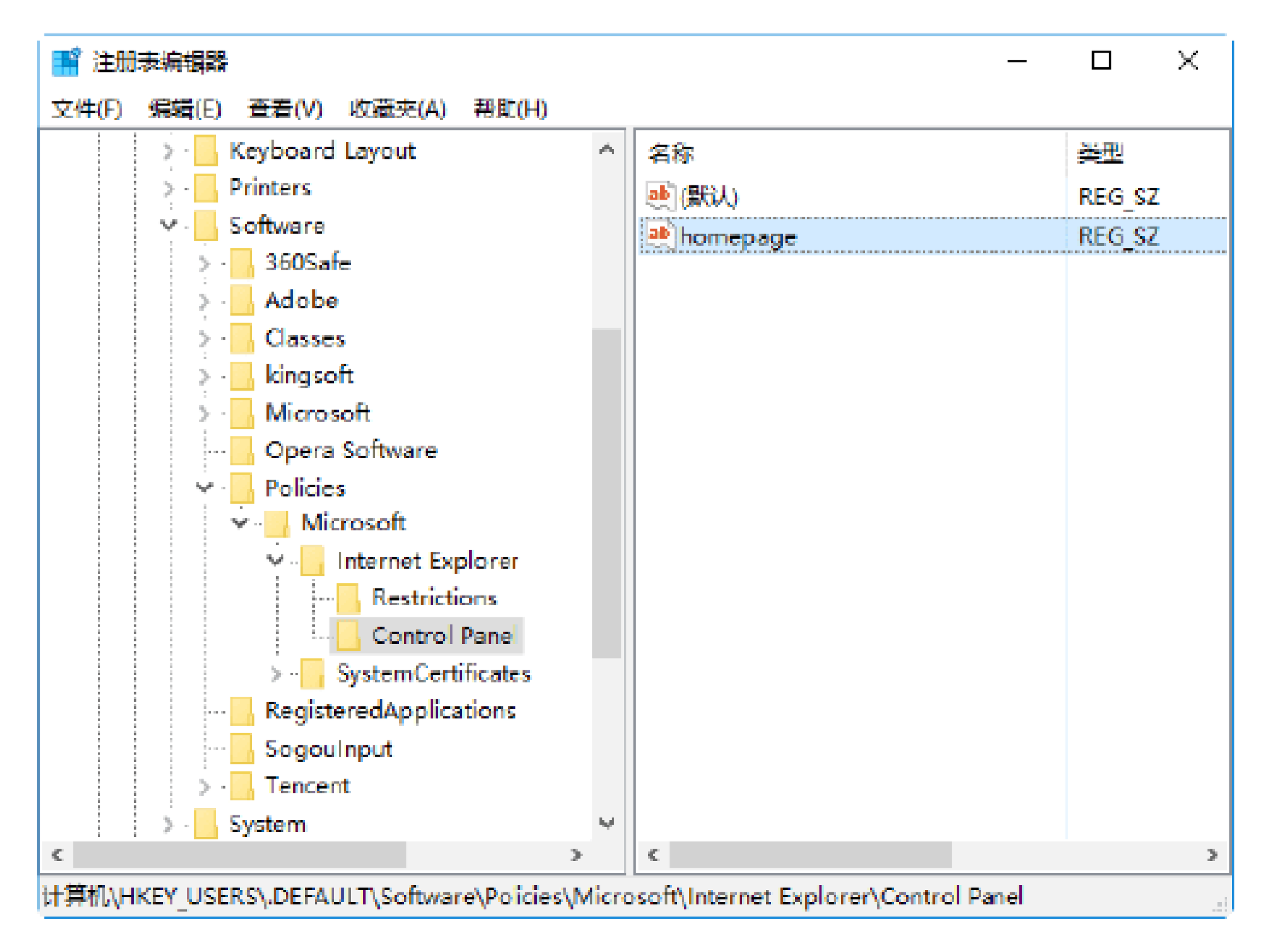


实战5：强行修改浏览器的首页按钮

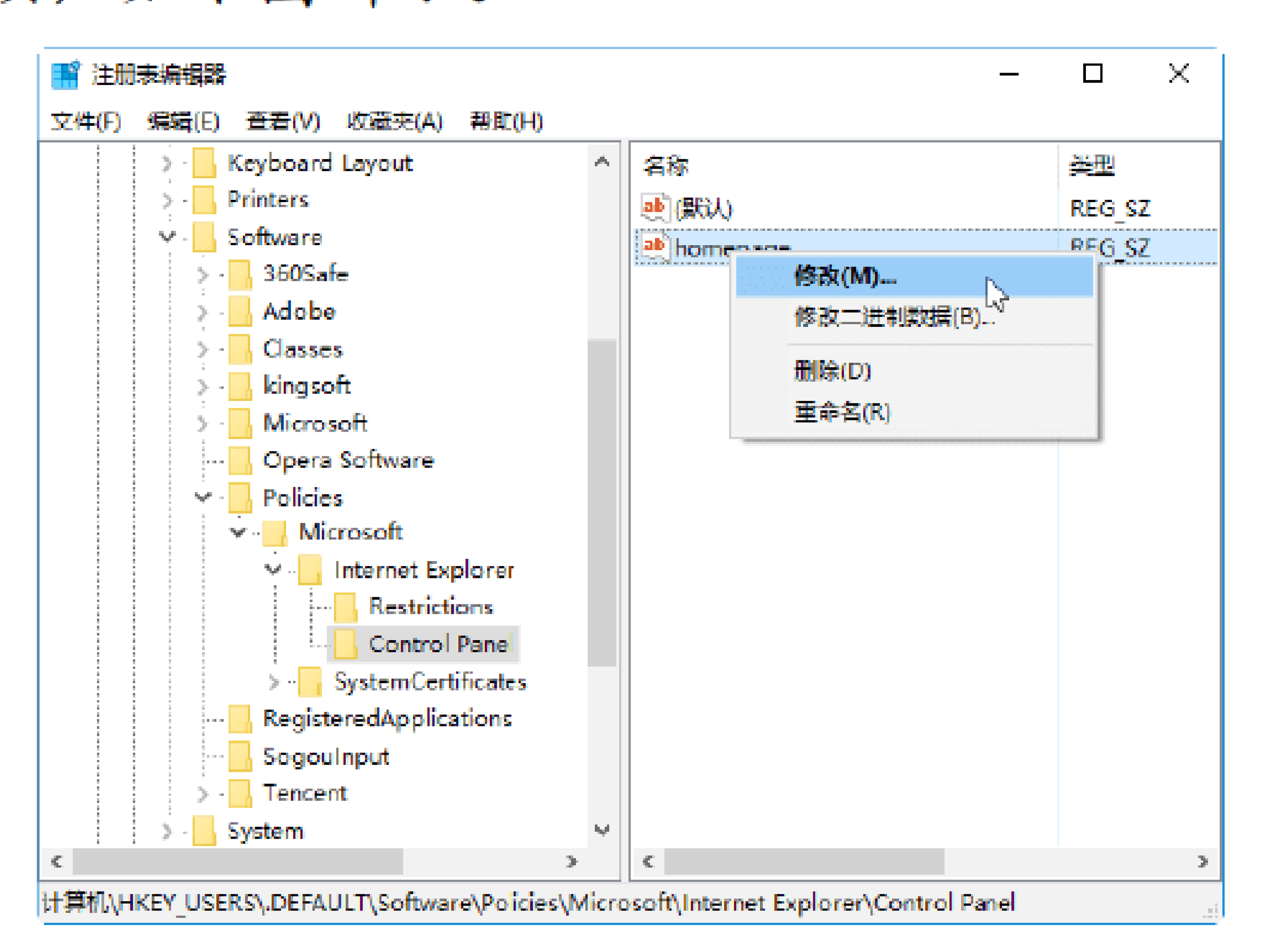
IE浏览器默认的首页变成灰色且按钮不可用，主要是由于注册表HKEY_USERS\.DEFAULT\Software\Policies\Microsoft\Internet Explorer\Control Panel下的homepage数值被修改的原因，即原来的数值为0，被修改为1。

针对这种情况，用户可以采用下列方法进行修复。

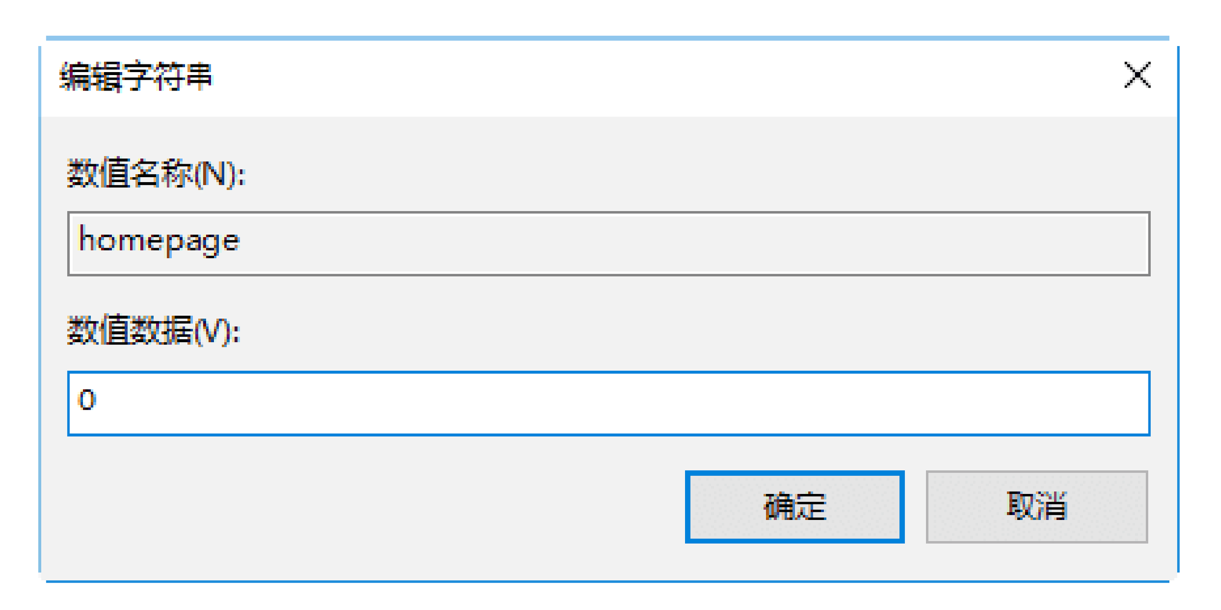
Step 01 打开"注册表编辑器"窗口，在左侧窗格中单击展开HKEY_USERS\.DEFAULT\Software\Policies\Microsoft\Internet Explorer\Control Panel，如下图所示。



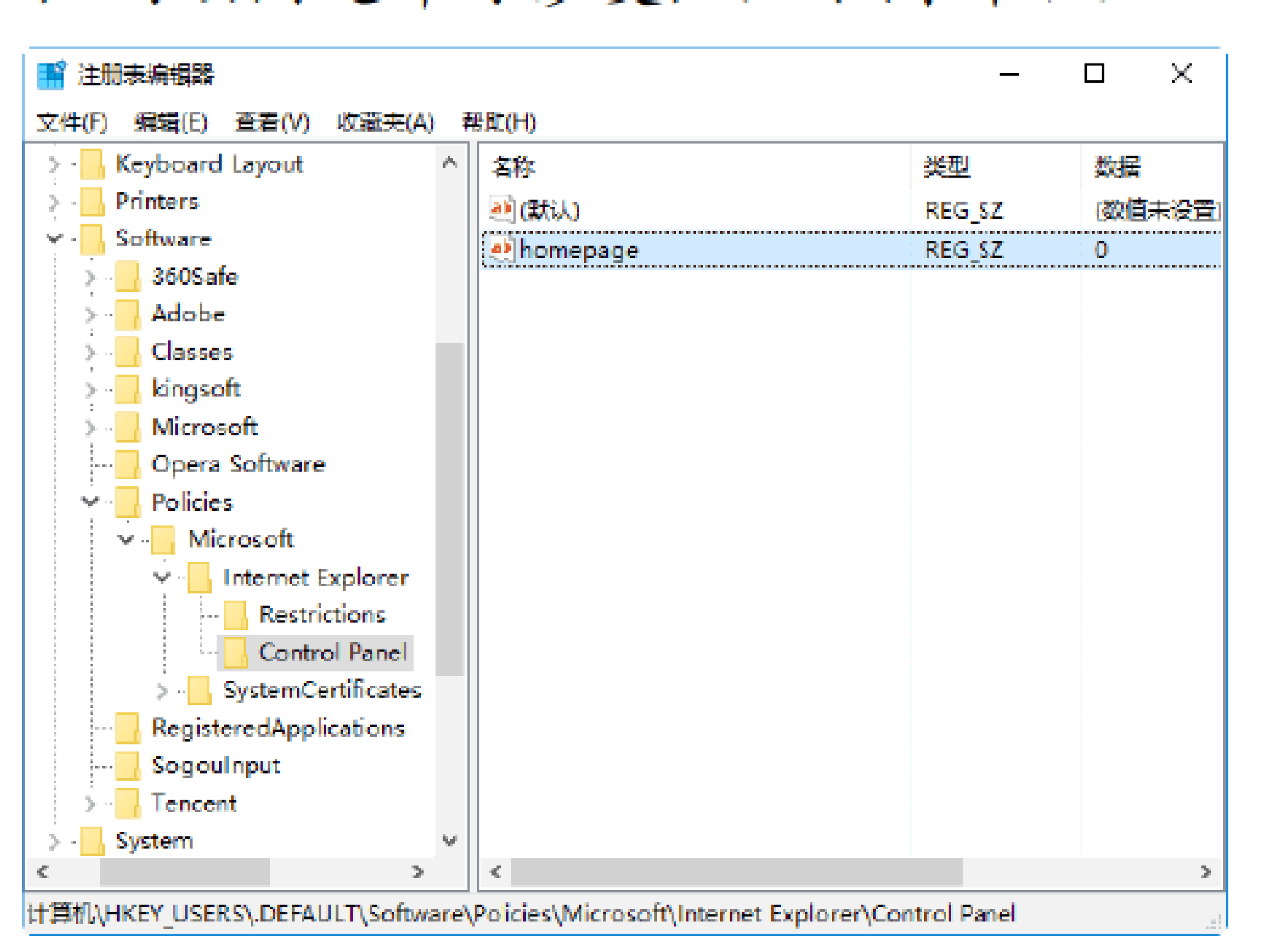
Step 02 在右侧窗格中选择homepage选项并右击，在弹出的快捷菜单中选择“修改”选项，如下图所示。



Step 03 打开“编辑字符串”对话框，在“数值数据”文本框中将数值“1”修改为“0”，如下图所示。



Step 04 单击“确定”按钮，重新启动计算机后，则该问题即可修复，如下图所示。



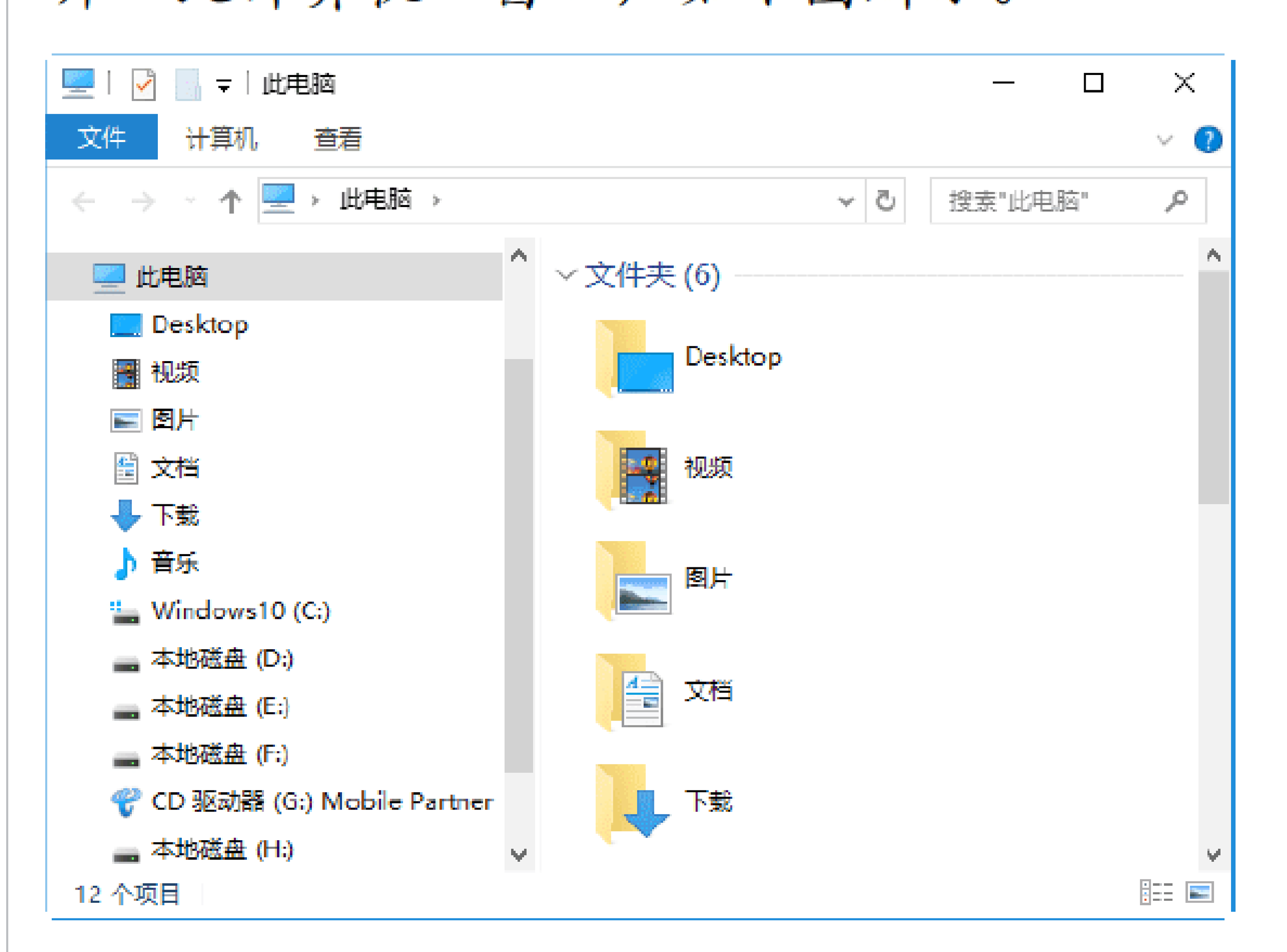
实战6：删除桌面上的浏览器图标



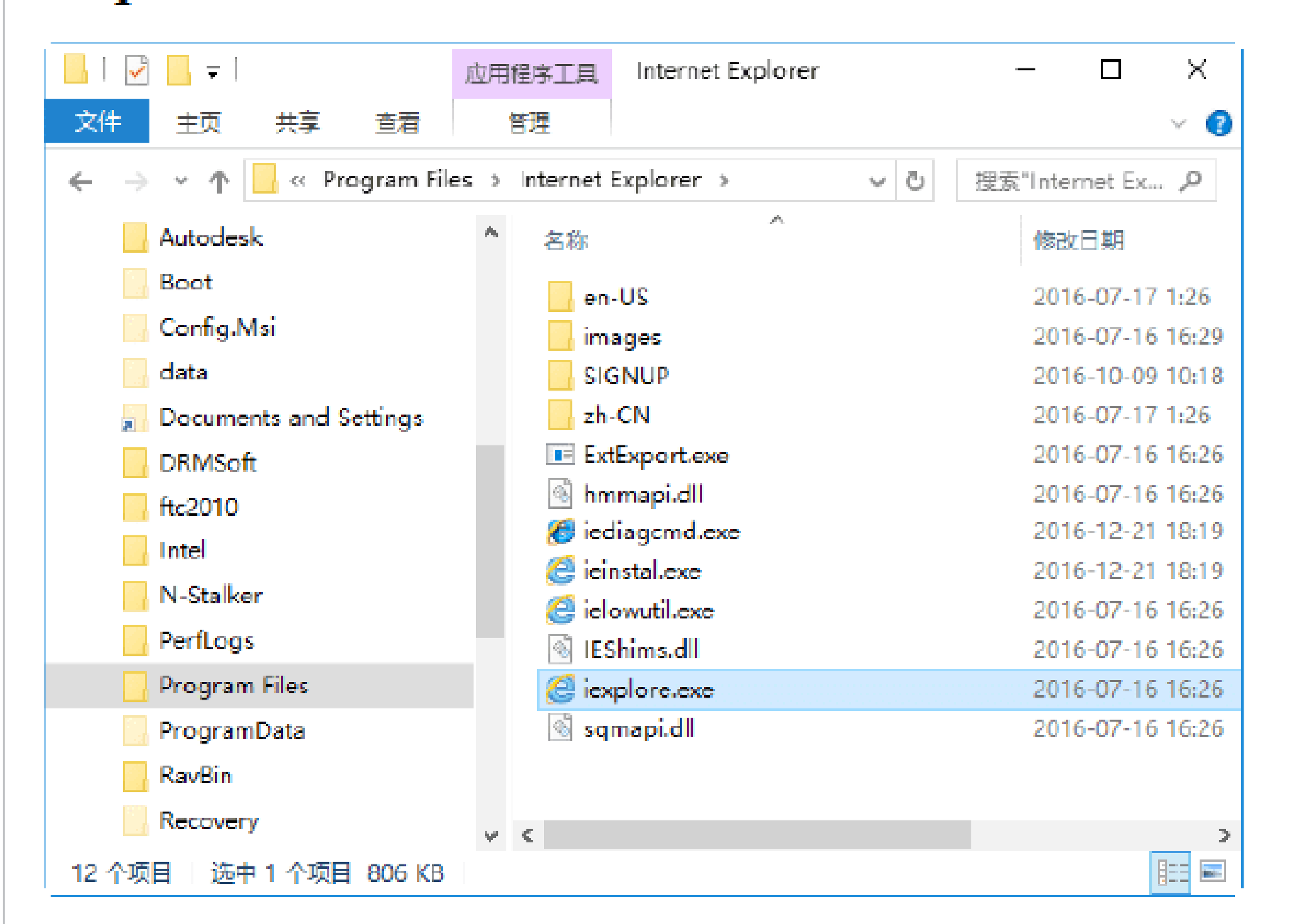
当桌面上的IE浏览器图标“不见”了，出现这种现象的主要原因还是流氓软件的篡改所致，或计算机中了病毒，这时建议用户使用杀毒软件查杀病毒，然后重新启动计算机。另外，还可以通过手动建立快捷方式使图标出现在桌面上。

通过手工建立IE快捷方式的具体操作步骤如下。

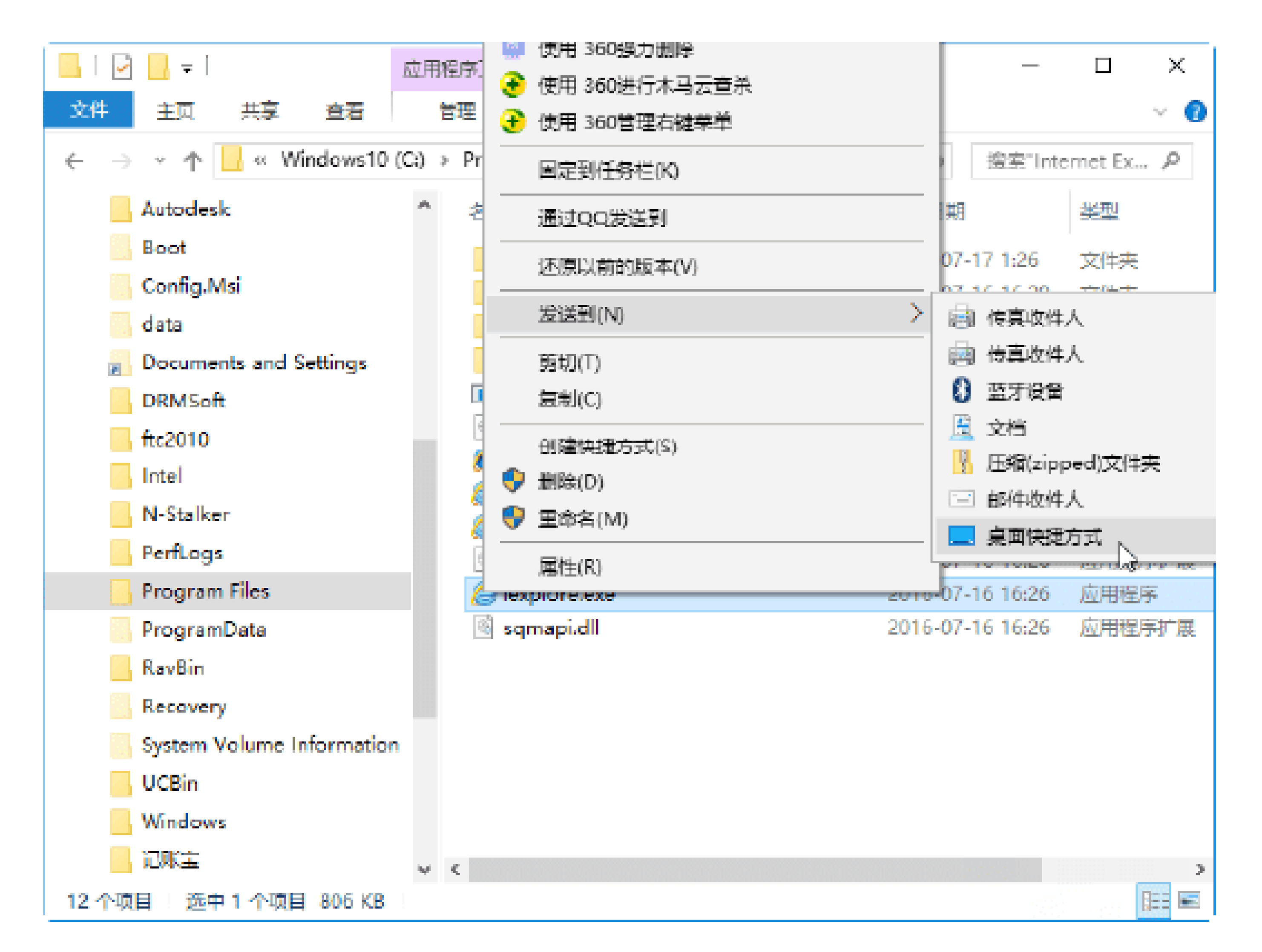
Step 01 双击桌面上的“此计算机”图标，打开“此计算机”窗口，如下图所示。



Step 02 在其中打开Program Files→ Internet Explorer文件夹，如下图所示。

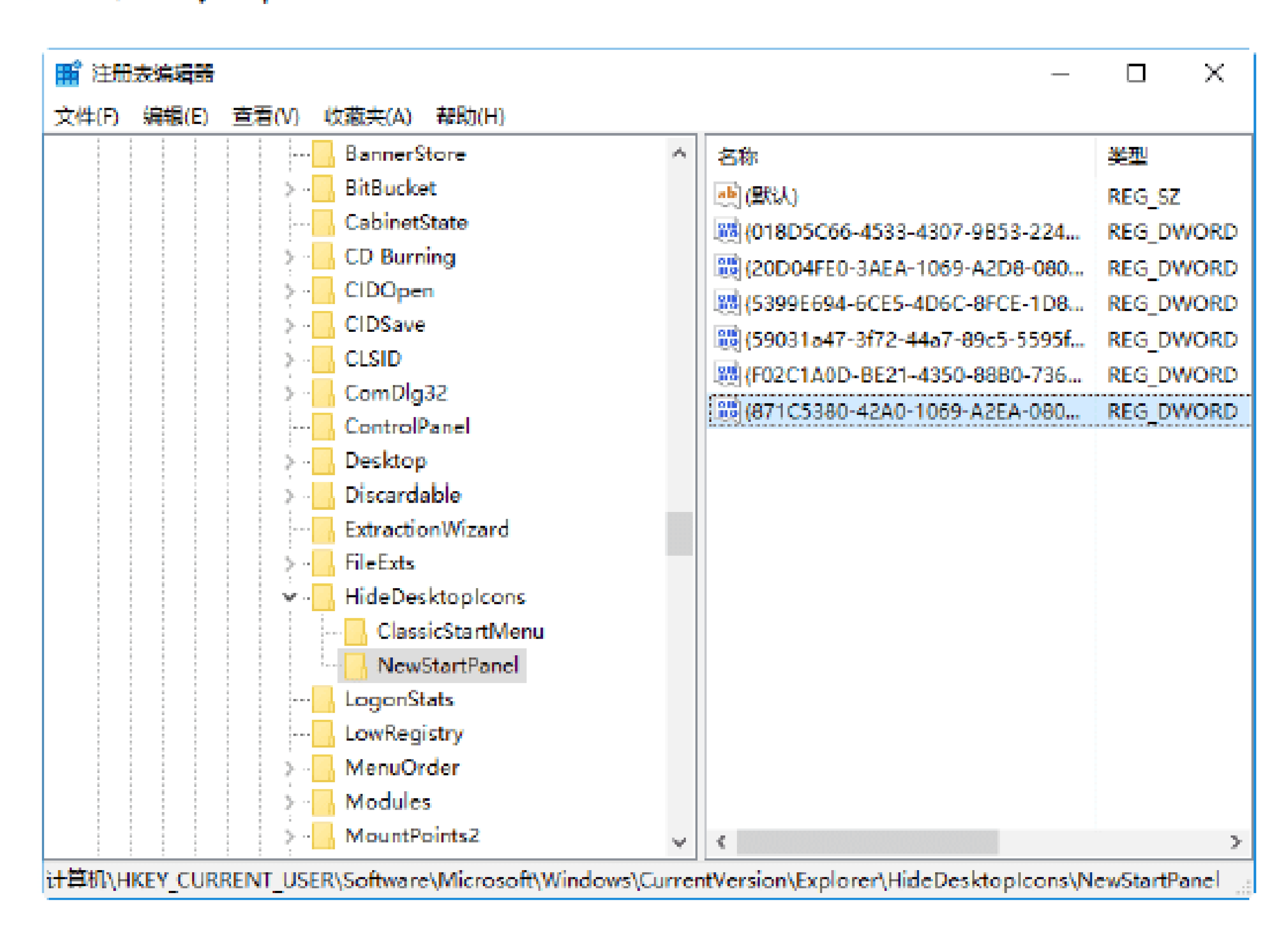


Step 03 选择iexplore.exe图标并右击，在弹出的快捷菜单中选择“发送到”→“桌面快捷方式”选项，这样就可以将IE快捷方式放到桌面上使用，如下图所示。



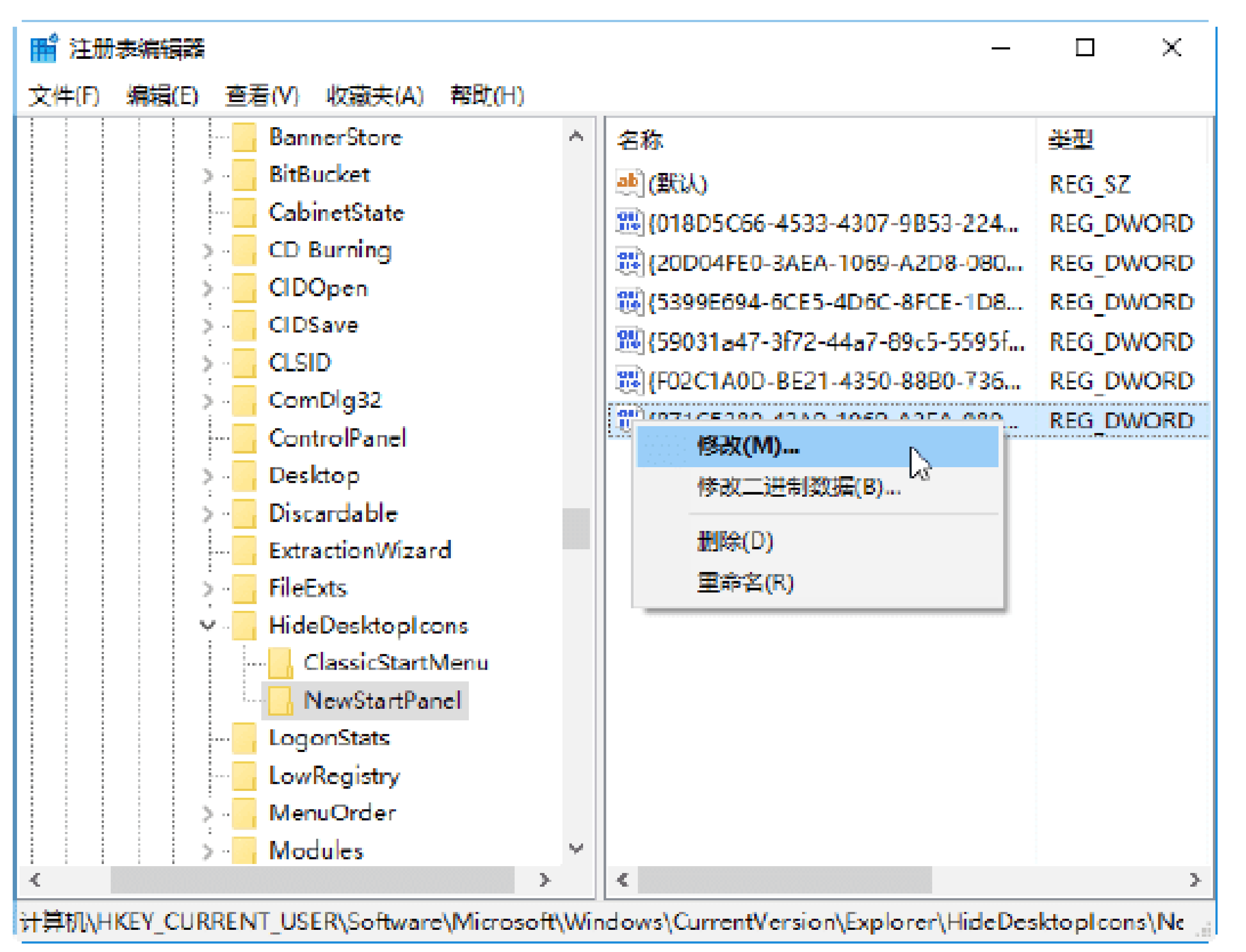
另外，还可以在注册表中修复IE浏览器图标“不见”的情况。具体的操作步骤如下。

Step 04 打开“注册表编辑器”，在左侧窗格中单击展开HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\HideDesktop-Icons \NewStartPanel，如下图所示。

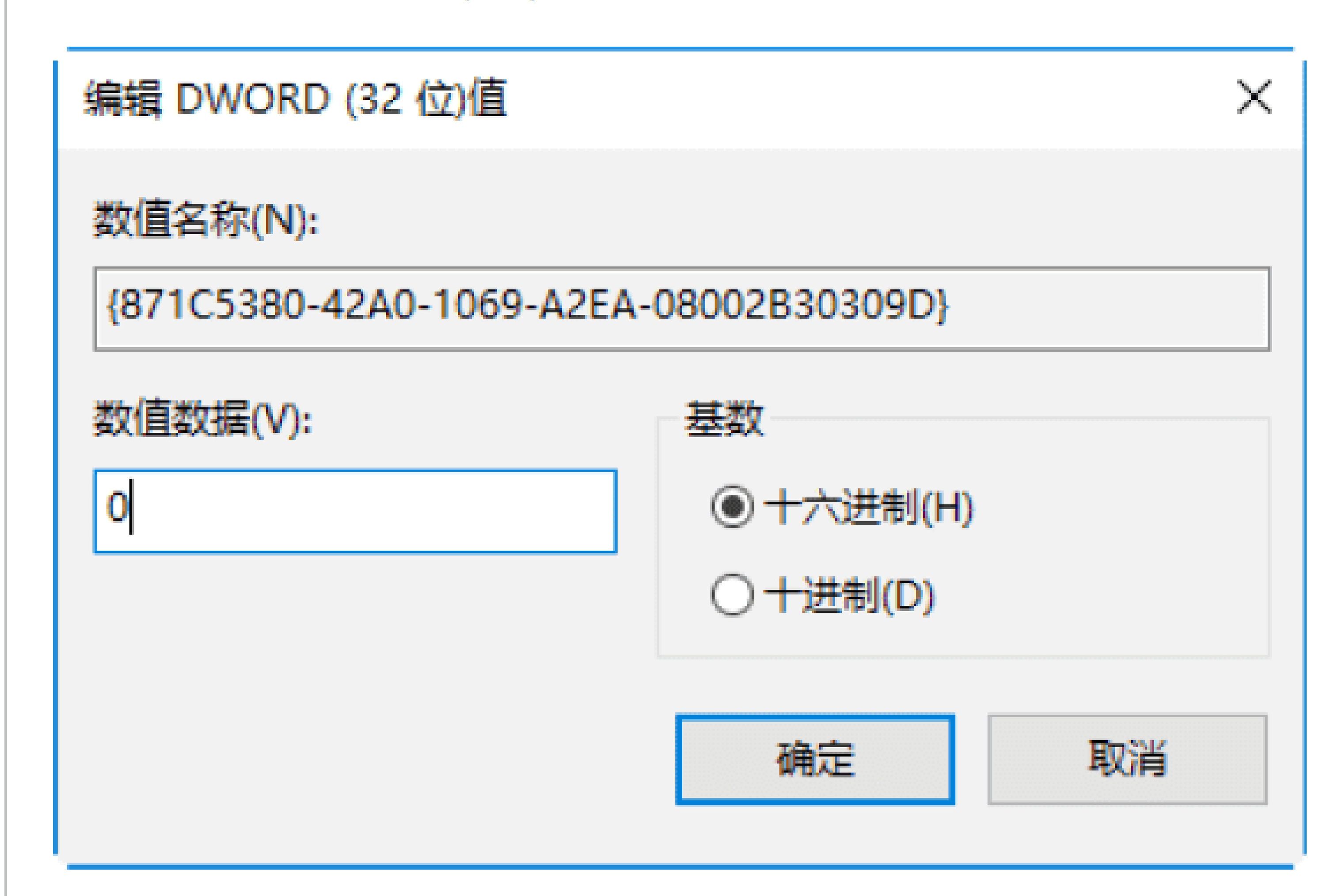


Step 05 在右侧的窗格中选择“871C5380-42A0-1069-A2EA-08002B30309D”键值项并右击，在弹出的快捷菜单中选择“修改”选项，如下图所示。

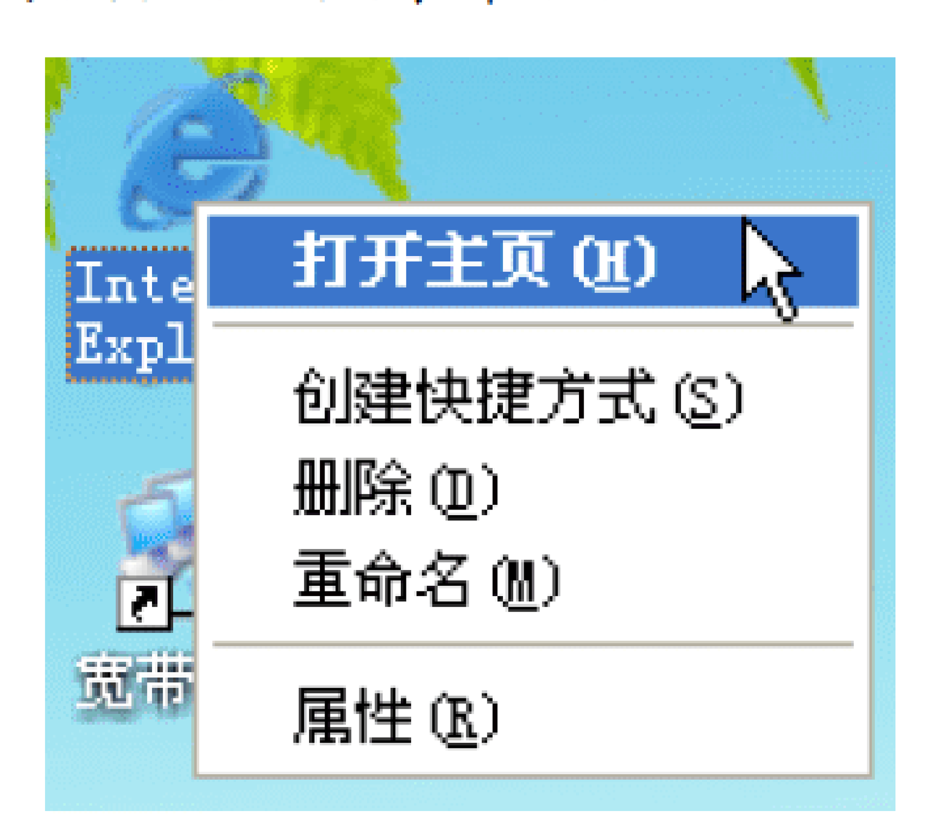




Step 06 打开“编辑DWORD（32位）值”对话框，在“数值数据”文本框中输入“0”，如下图所示。



Step 07 单击“确定”按钮，然后刷新桌面，即可看到消失的IE图标重新出现，且右键菜单也可用，如下图所示。



8.2 IE浏览器的自我安全防护

为保护计算机的安全，在上网浏览网页时需要注意对网页浏览器的安全维护，一般情况下，网页浏览器自身均有防护功能。这里以最常用的IE浏览器为例，介绍网页浏览器的自身防护技巧。

实战7：提高IE的安全防护等级

通过设置IE浏览器的安全等级，可以防止用户打开含有病毒和木马程序的网页，这样可以保护系统和计算机的安全。具体操作步骤如下。

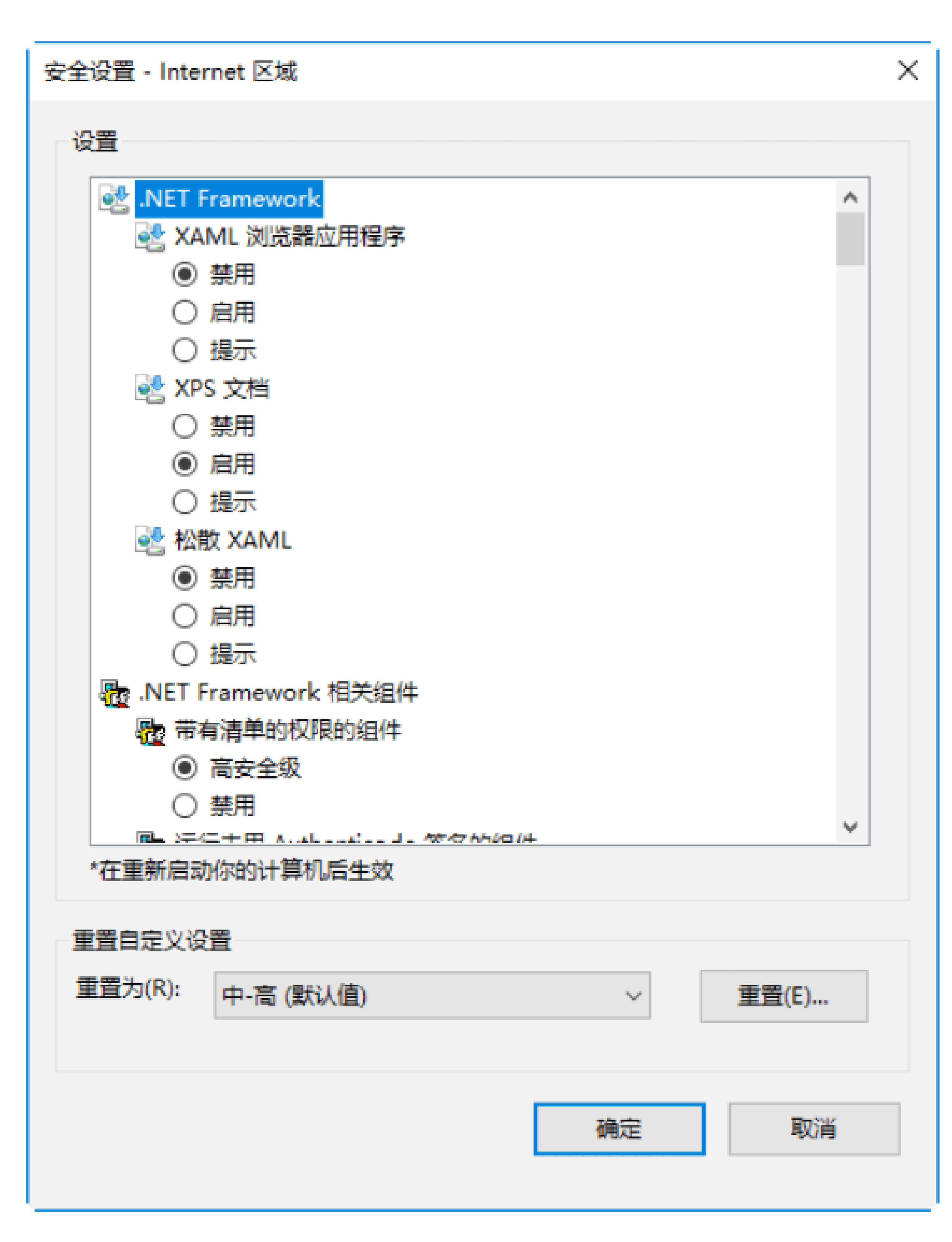
Step 01 在IE浏览器中选择“工具”→“Internet选项”选项，打开“Internet选项”对话框，如下图所示。



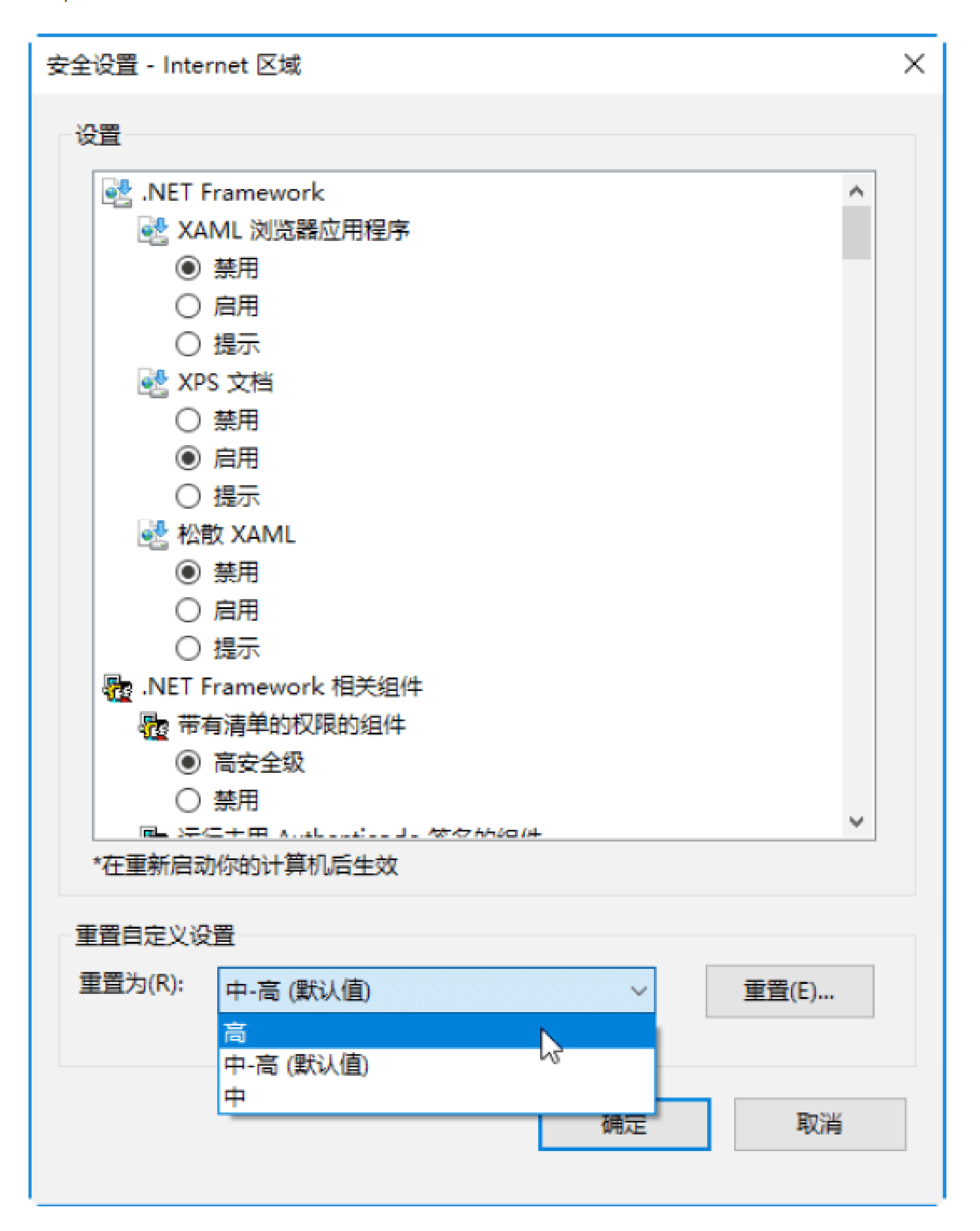
Step 02 选择“安全”选项卡，进入“安全”设置界面，如下图所示。



Step 03 选中Internet图标，单击“自定义级别”按钮，打开“安全设置”对话框，如下图所示。



Step 04 单击“重置为”下拉按钮，在弹出的下拉列表中选择“高”选项，如下图所示。



Step 05 单击“确定”按钮，即可将IE安全等级设置为“高”，如下图所示。

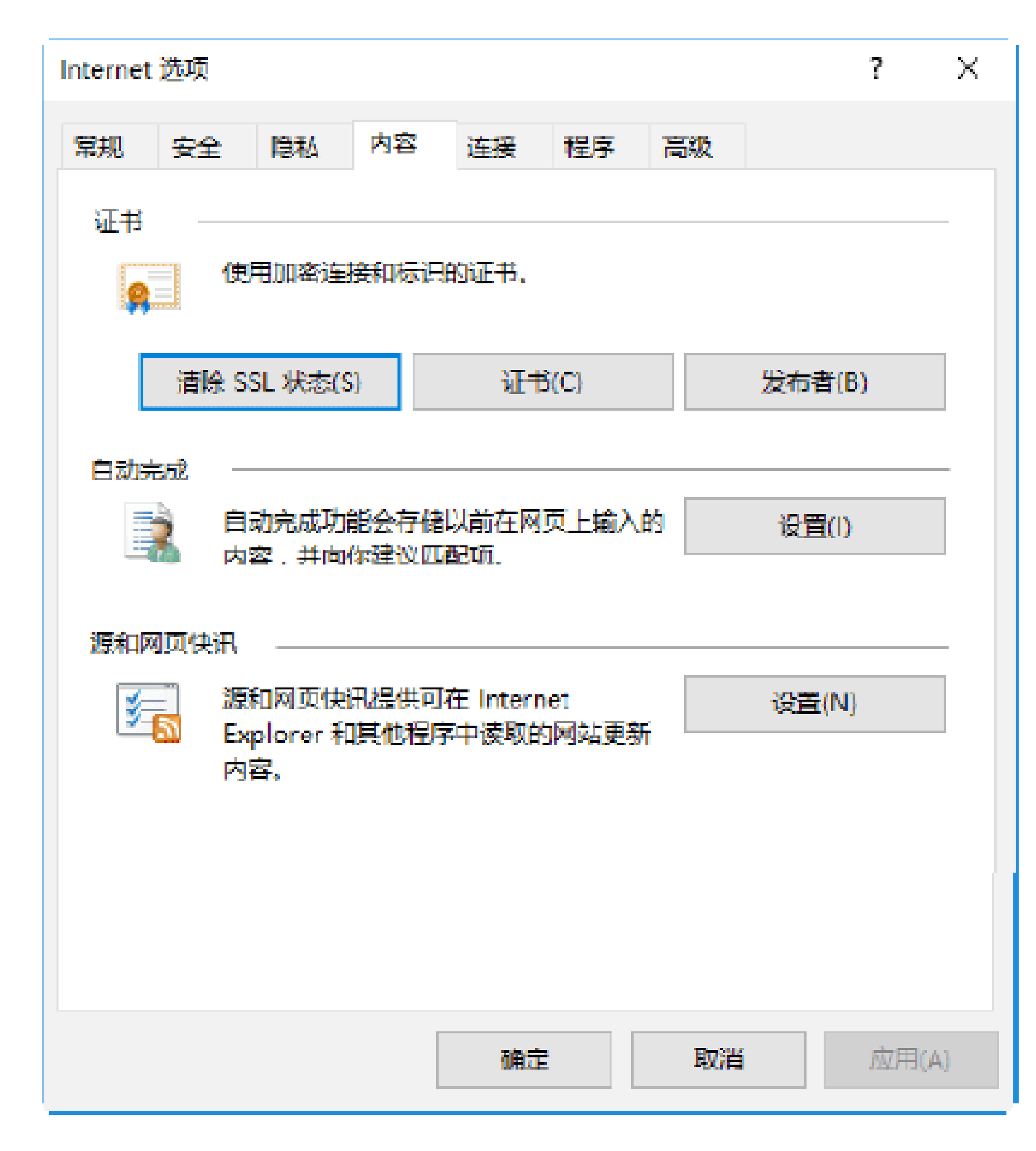


实战8：清除浏览器中的表单信息

浏览器的表单功能在一定程度上方便了用户，但也被黑客用来窃取用户的数据信息，所以从安全角度出发，需要清除浏览器的表单并取消自动记录表单的功能。

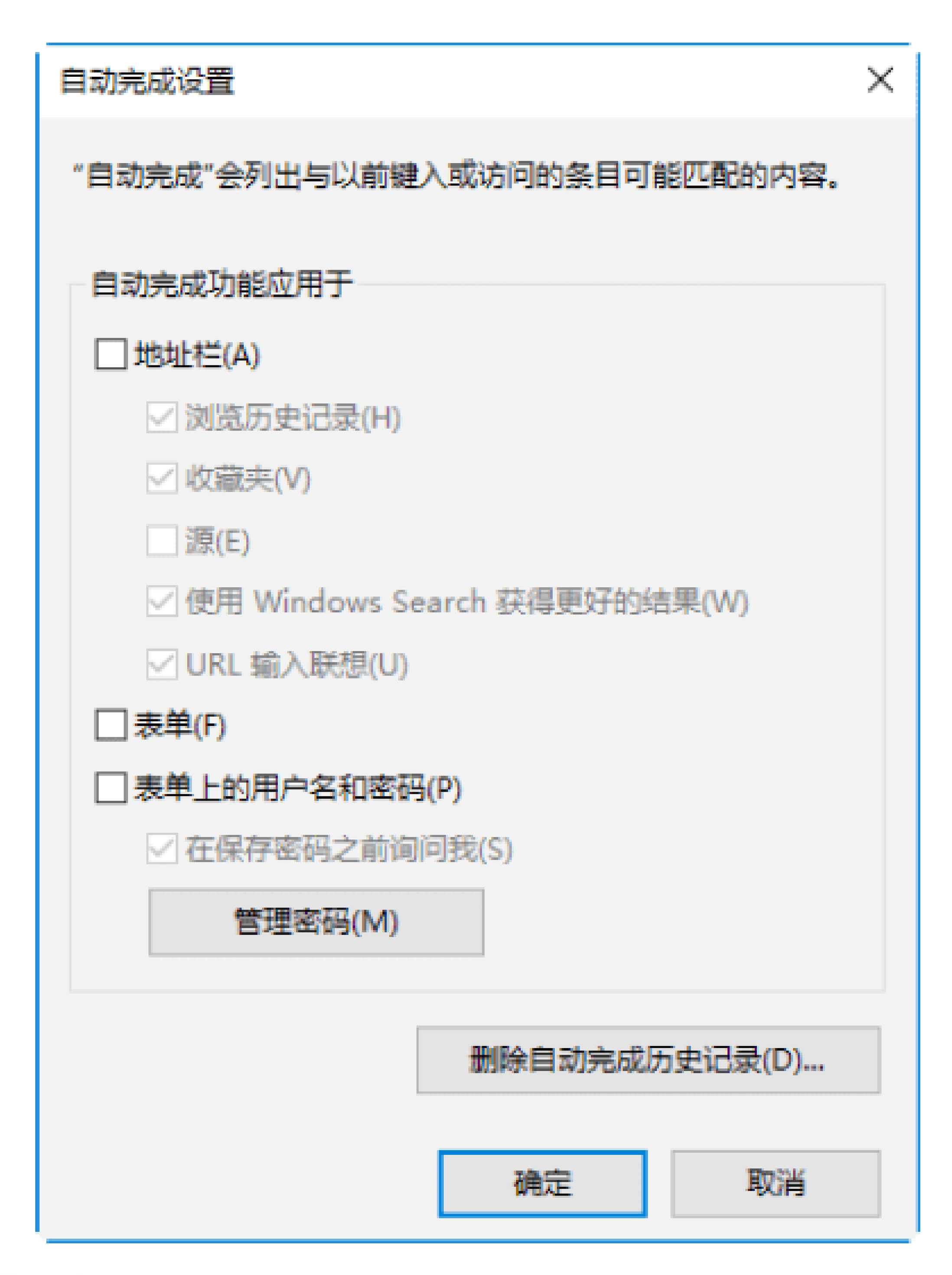
清除IE浏览器中表单的具体操作步骤如下。

Step 01 在IE浏览器中选择“工具”→“Internet选项”选项，打开“Internet选项”对话框，选择“内容”选项卡，如下图所示。

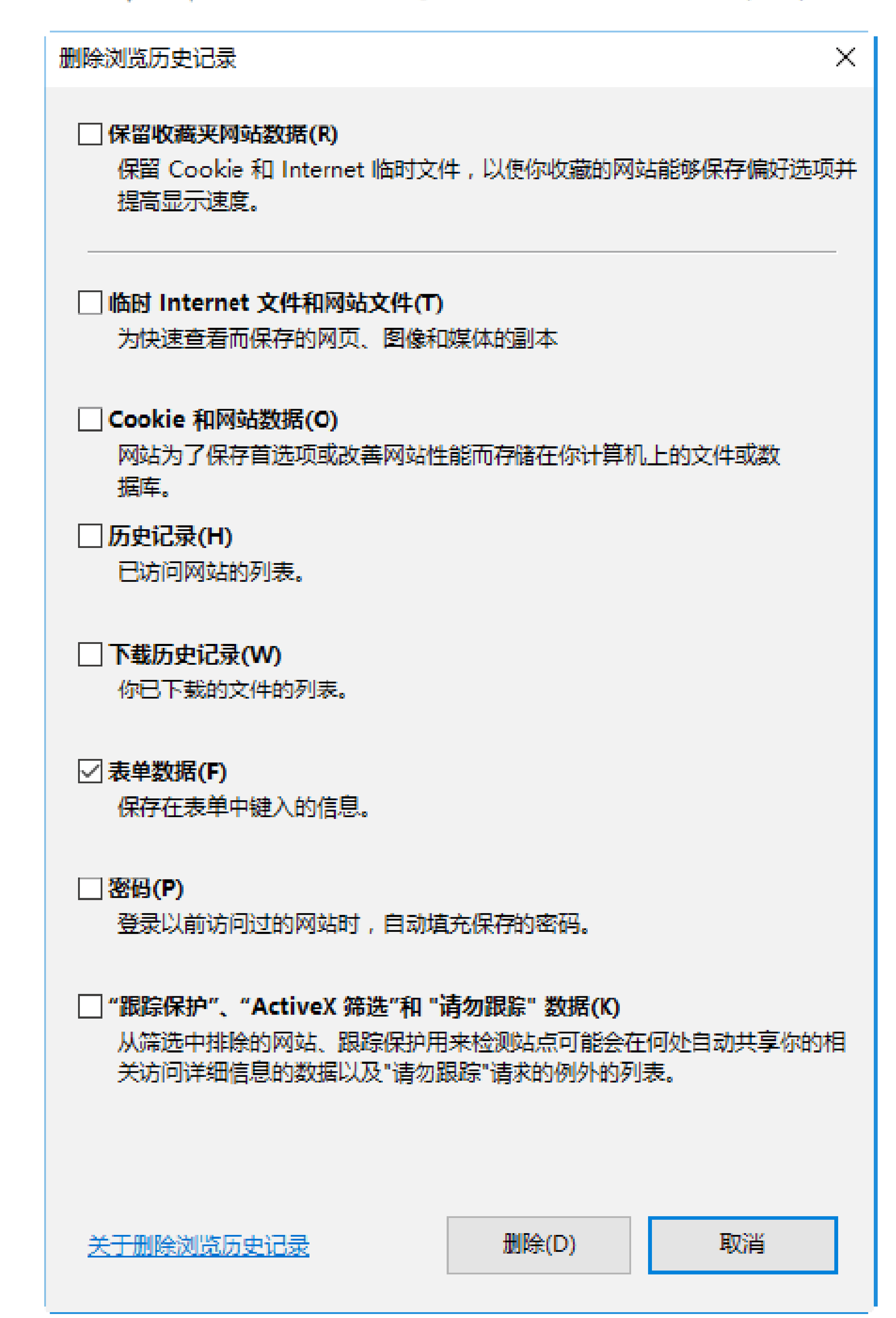




Step 02 在“自动完成”选项区域中单击“设置”按钮，打开“自动完成设置”对话框，取消勾选所有的复选框，如下图所示。



Step 03 单击“删除自动完成历史记录”按钮，打开“删除浏览历史记录”对话框，勾选“表单数据”复选框，如下图所示。



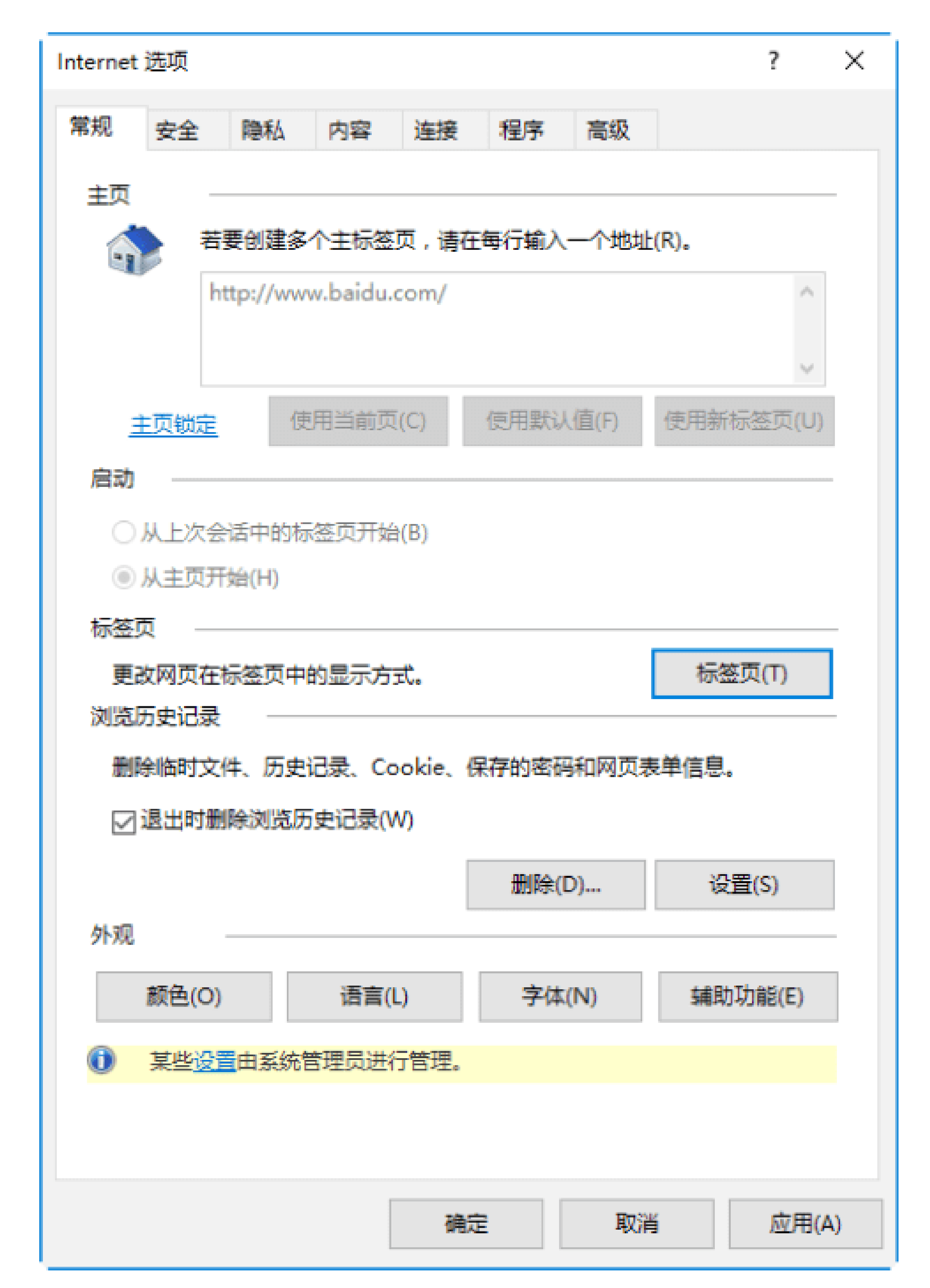
Step 04 单击“删除”按钮，即可删除浏览器中的表单信息。

实战9：清除浏览器的上网历史记录

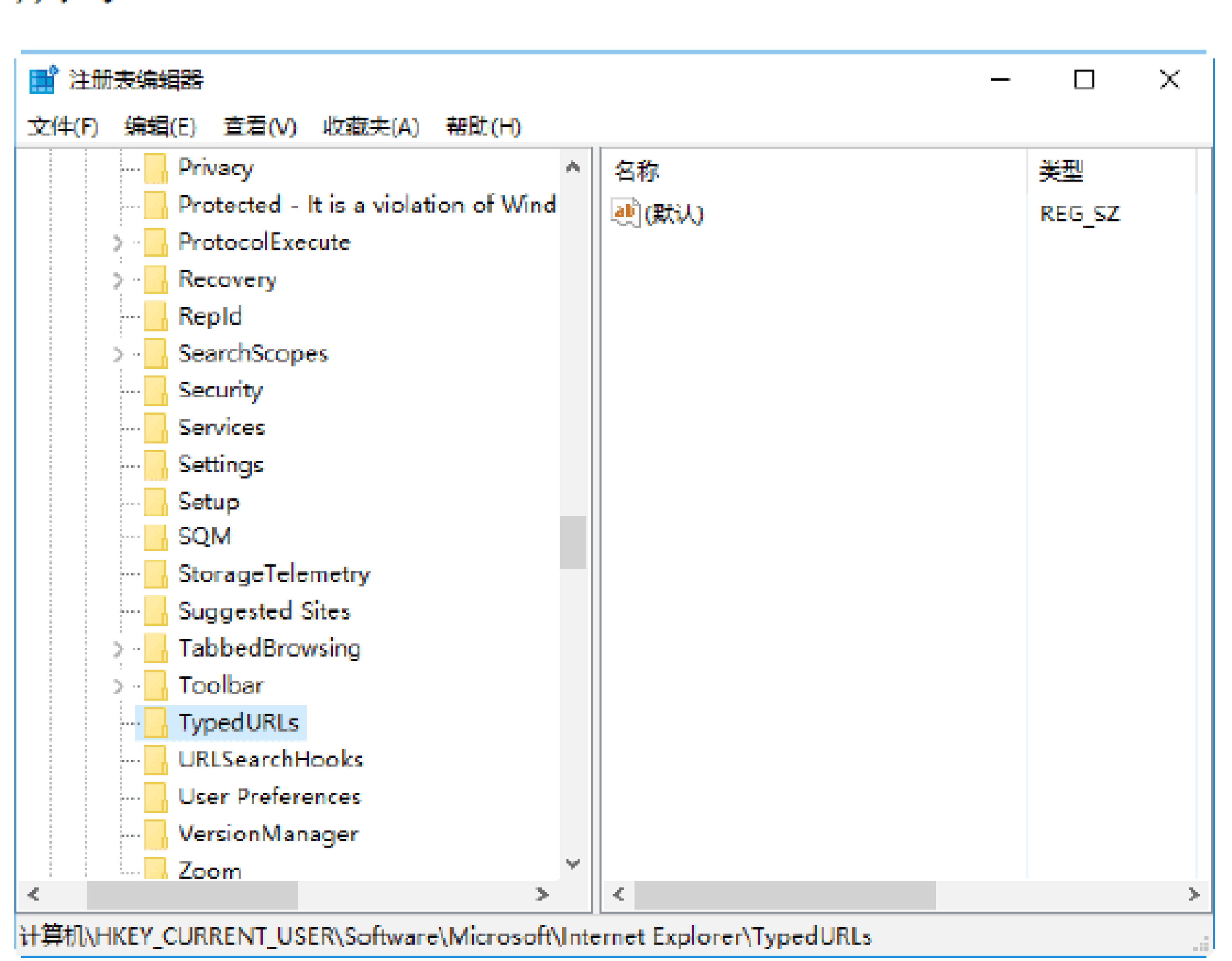
Windows操作系统具有历史记录功能，可以将用户以前所运行过的程序、浏览过的网站、查找过的内容等记录下来，但这同样会泄露用户的信息。

可以通过以下方法对这些信息进行清除。

方法1：在“Internet 选项”对话框的“常规”选项卡中，勾选“浏览历史记录”区域中的“退出时删除浏览历史记录”复选框，即可实现清除浏览过的IE网址，如下图所示。



方法2：利用注册表进行清除。IE历史记录在“注册表编辑器”中的保存位置是HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs，因此，只要删除该子项下的所有内容即可，如下图所示。



提示：在输入网址时按下Ctrl+O组合键，在弹出的“打开”对话框中填入要访问的网站名称或IP地址，输入的地址链接URL就不会保存在地址栏里了。

实战10：删除上网Cookie信息



Cookie是Web服务器发送到计算机里的数据文件，它记录了用户名、口令及其他一些信息。特别目前在许多网站中，Cookie文件中的Username和Password是不加密的明文信息，就更容易泄密。因此，在离开时删除Cookie内容是非常必要的。

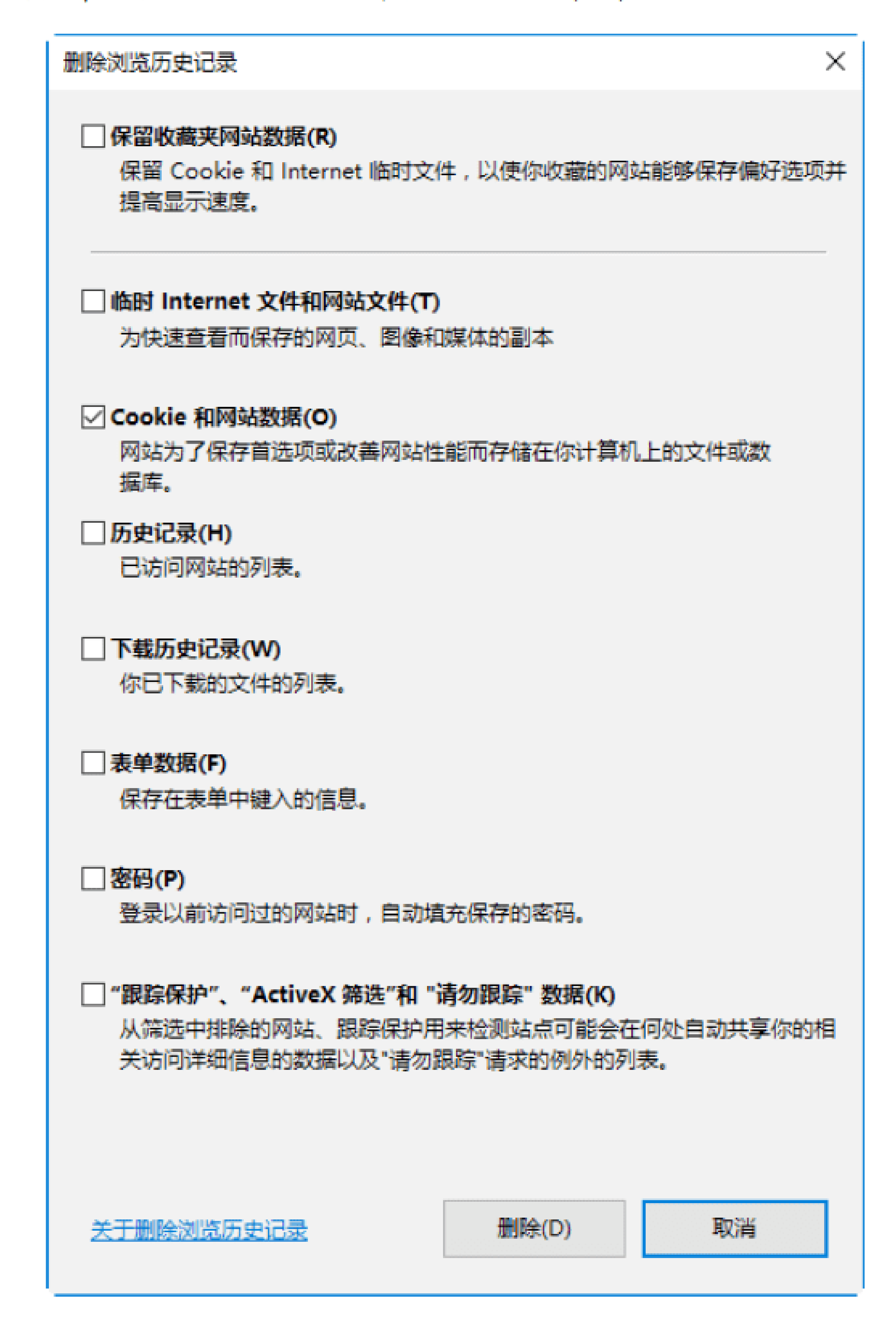
用户可以通过“Internet选项”对话框中的相关功能实现删除Cookies。具体的操作步骤如下。

Step 01 打开“Internet选项”对话框，选择“常规”选项卡，在“浏览历史记录”选项区域中单击“删除”按钮，如下图所示。



Step 02 打开“删除浏览历史记录”对话框，在其中勾选“Cookies和网站数据”复选

框，单击“删除”按钮，即可清除IE浏览器中的Cookies文件，如下图所示。



8.3 Microsoft Edge浏览器的自我安全防护

通过Microsoft Edge浏览器用户可以浏览网页，还可以根据自己的需要设置其他功能，如在阅读视图模式下浏览网页、将网页添加到浏览器的收藏夹中、给网页做Web笔记等。



实战11：Microsoft Edge基本操作

Microsoft Edge基本操作包括启动、关闭与打开网页等，下面分别进行介绍。

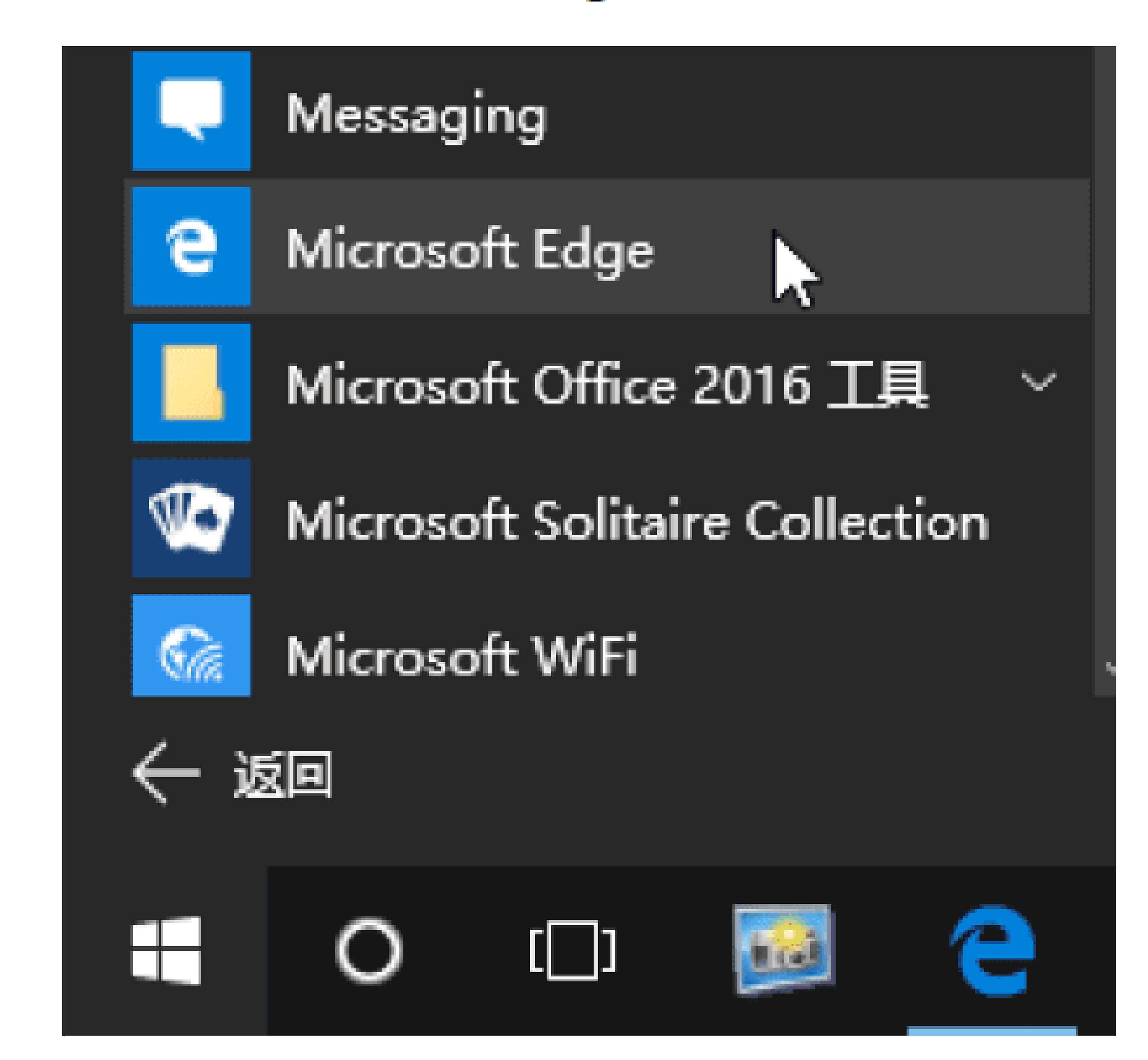
1. 启动Microsoft Edge浏览器

启动Microsoft Edge浏览器，通常使用以下3种方法之一：

（1）双击桌面上的Microsoft Edge快捷方式图标；

（2）单击快速启动栏中的Microsoft Edge图标；

（3）单击“开始”按钮，选择“所有程序”→Microsoft Edge选项。



通过上述3种方法之一打开Microsoft Edge浏览器。默认情况下，启动Microsoft Edge后将会打开用户设置的首页，它是用户进入因特网的起点。如下图所示用户设置的首页为百度搜索页面。



2. 使用Microsoft Edge浏览器打开网页

如果知道要访问网页的网址（即URL），则可以直接在Microsoft Edge浏览器中的地址栏中输入该网址，然后按Enter键，即可打开该网页。例如，在地址栏中输入新浪网网址http://www.sina.com.cn/，按Enter键，即可进入该网站的首页。



另外，当打开多个网页后，单击地址栏中的下拉按钮，在弹出的下拉列表中可以看到曾经输入过的网址。当在地址栏中再次输入该地址时，只需要输入一个或几个字符，地址栏中将自动弹出一个下拉列表，其中列出了与输入部分相同的曾经访问过的所有网址，在其中选择所需要的网址，即可进入相应的网页，如下图所示。



3.关闭Microsoft Edge浏览器

当用户浏览网页结束后，就需要关闭Microsoft Edge浏览器，同大多数Windows应用程序一样，关闭Microsoft Edge浏览器通常采用以下3种方法之一：

（1）单击“Microsoft Edge浏览器”窗口右上角的“关闭”按钮 × ；

（2）按Alt+F4组合键；

（3）右击Microsoft Edge浏览器的标题栏，在弹出的快捷菜单中选择“关闭”选项。

为了方便起见，用户一般采用第一种方法来关闭Microsoft Edge浏览器。



实战12：在阅读视图模式下浏览网页



Microsoft Edge浏览器提供阅读视图模式，可以在没有干扰（没有广告，没有网页的头标题和尾标题等，只有正文）的模式下阅读文章，还可以调整背景和文字大小。具体的操作步骤如下。

Step 01 在Microsoft Edge浏览器中，打开一篇文章的网页，如这里打开一篇有关“蜂蜜”介绍的网页，单击浏览器工具栏的“阅读视图”按钮 ，如下图所示。



Step 02 进入网页“阅读视图”模式中，可以看到此模式下除了文章之外，没有网页上其他的东西，如下图所示。

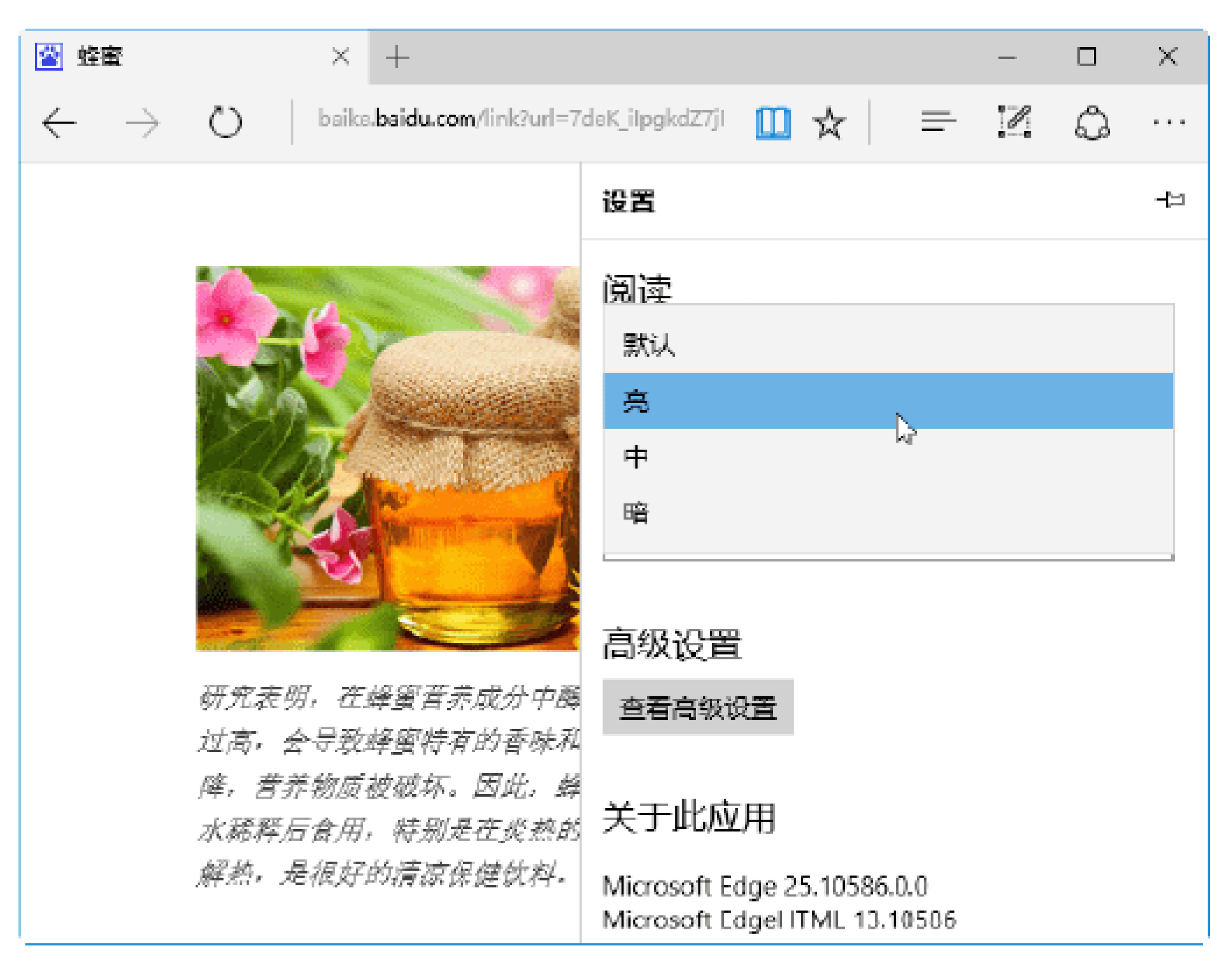


提示：再次单击“阅读视图”按钮，可退出阅读模式。

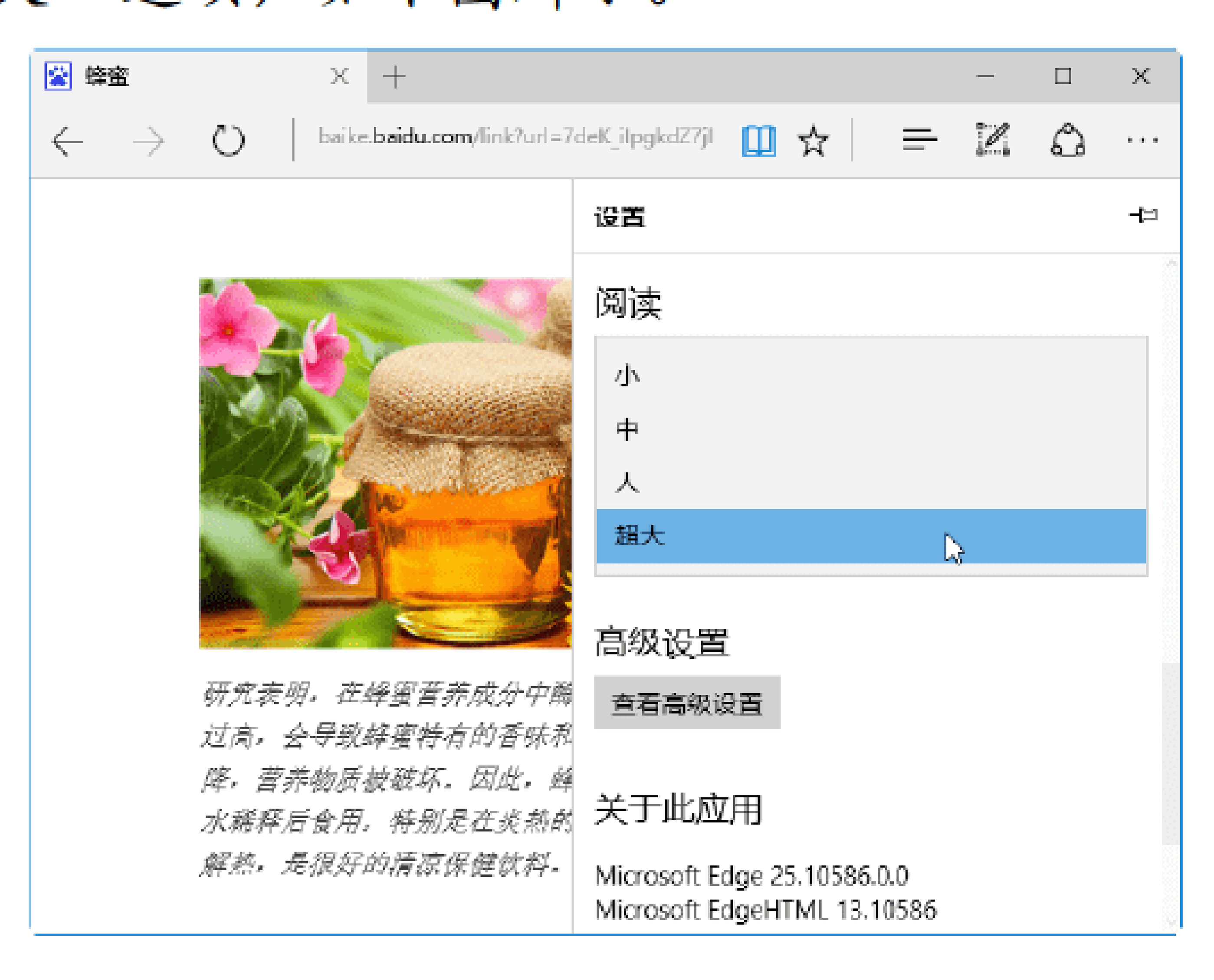
Step 03 如果想调整阅读时的背景和字体大小，需要单击浏览器中的“更多”按钮，在弹出的下拉列表中选择“设置”选项，如下图所示。



Step 04 打开“设置”界面，单击“阅读”视图“风格”下方的下拉按钮，在弹出的下拉列表中选择“亮”选项，如下图所示。



Step 05 单击“阅读”视图“字号”下方的下拉按钮，在弹出的下拉列表中选择“超大”选项，如下图所示。



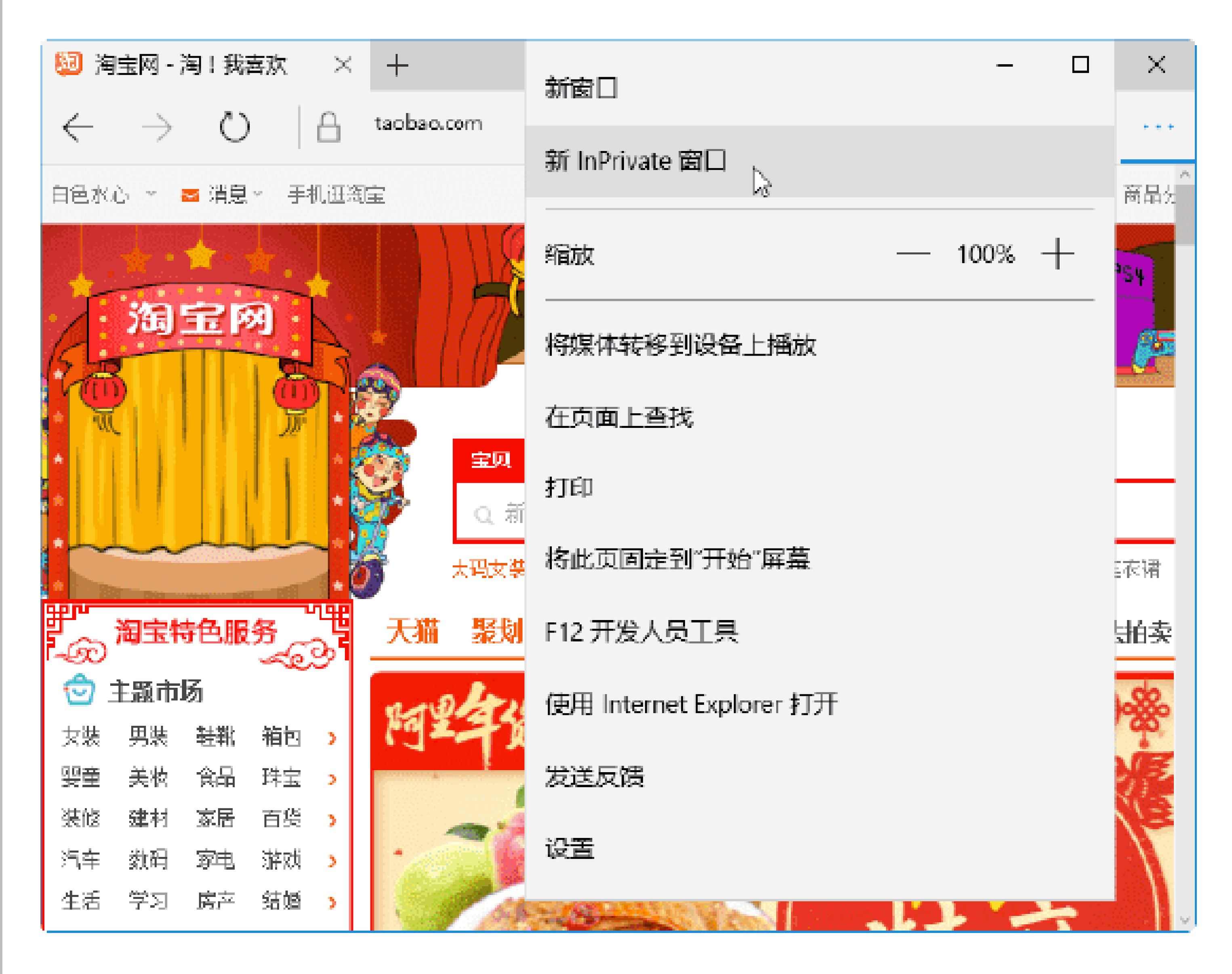
Step 06 设置完毕后，返回到“阅读视图”中，可以看到调整设置后的效果，如下图所示。



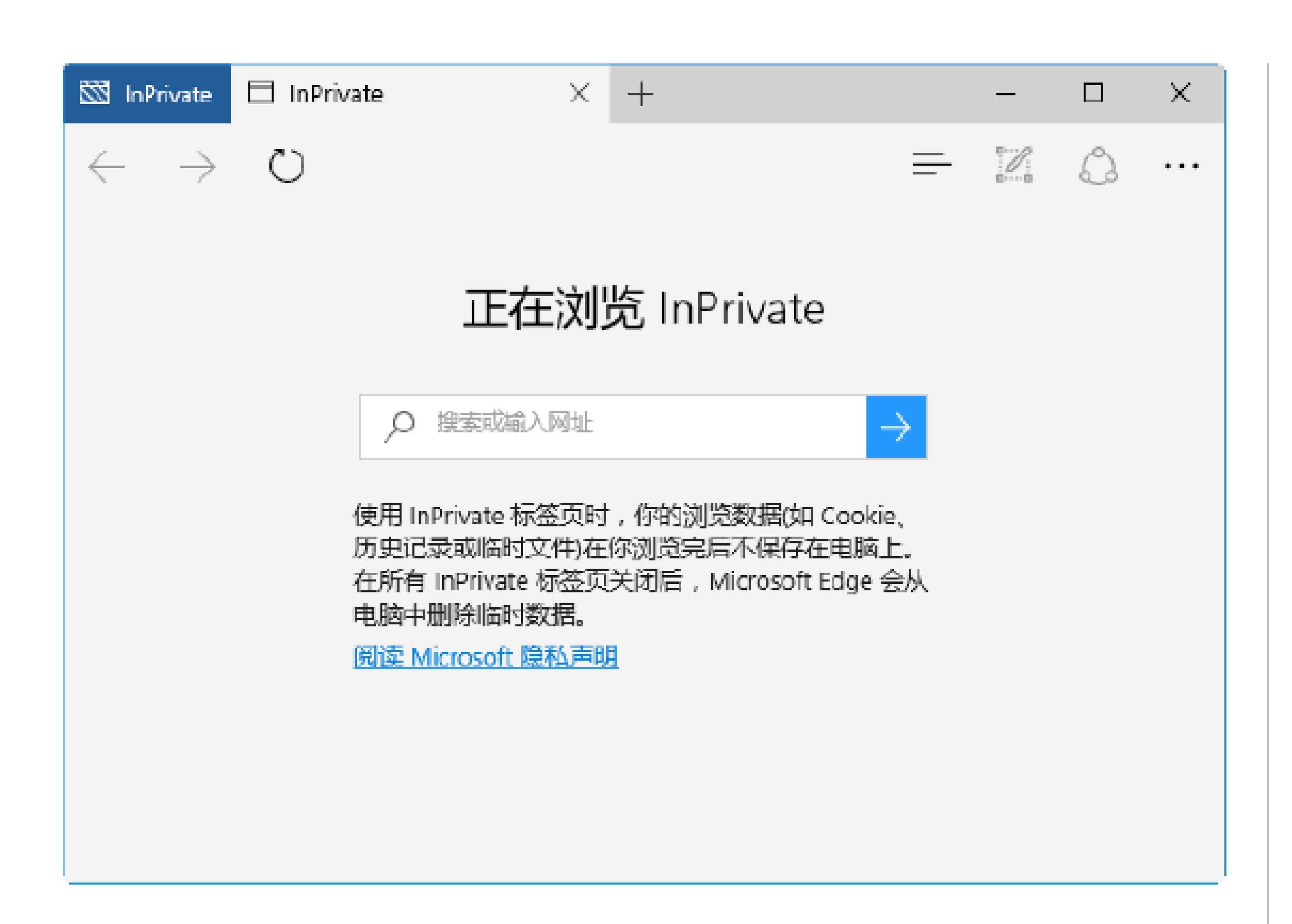
实战13：使用InPrivate浏览网页信息

使用InPrivate浏览网页时，用户的浏览数据（如Cookie、历史记录或临时文件）在用户浏览后不保存在计算机上。也就是说，当关闭所有的InPrivate标签页后，Microsoft Edge会从计算机中删除临时数据。使用InPrivate浏览网页的操作步骤如下。

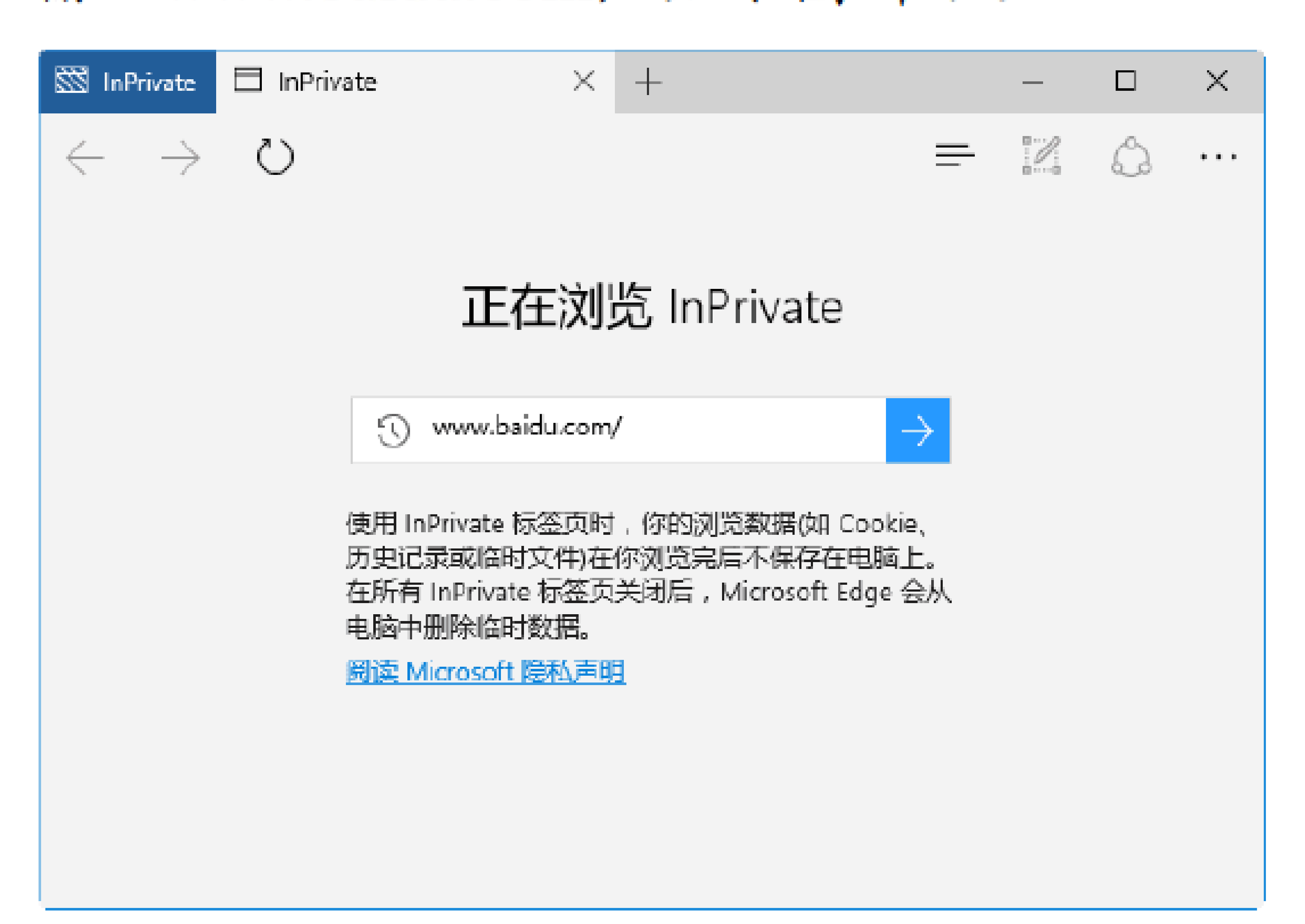
Step 01 双击任务栏中的Microsoft Edge图标，打开Microsoft Edge浏览工作界面，单击“更多”按钮，在弹出的下拉列表中选择“新InPrivate窗口”选项，如下图所示。



Step 02 打开InPrivate窗口，在其中提示用户正在浏览InPrivate，如下图所示。



Step 03 在“搜索或输入网址”文本框中输入想要使用InPrivate浏览的网页网址，如这里输入www.baidu.com，如下图所示。



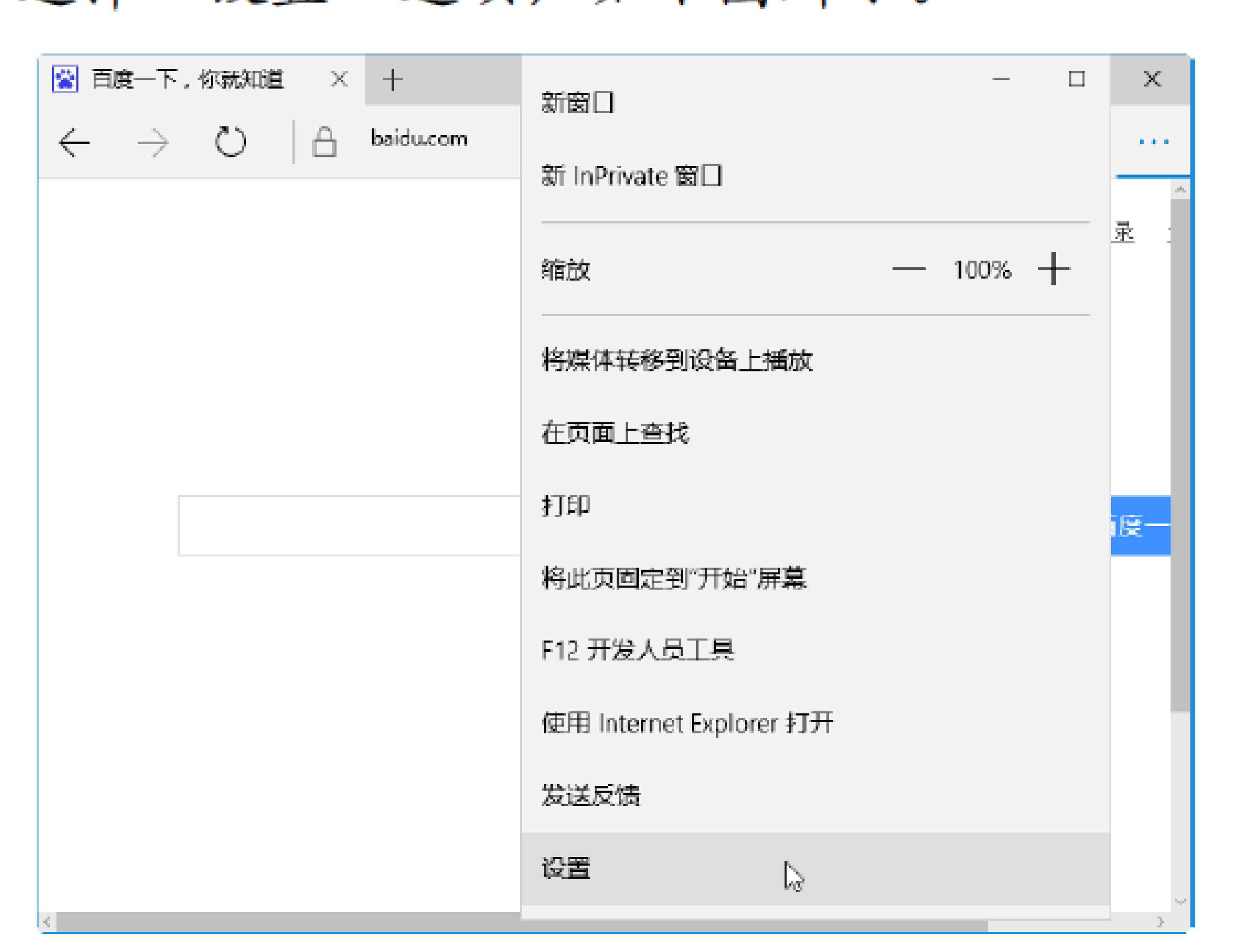
Step 04 单击“→”按钮，即可在InPrivate中打开百度网首页，进而浏览网页，如下图所示。



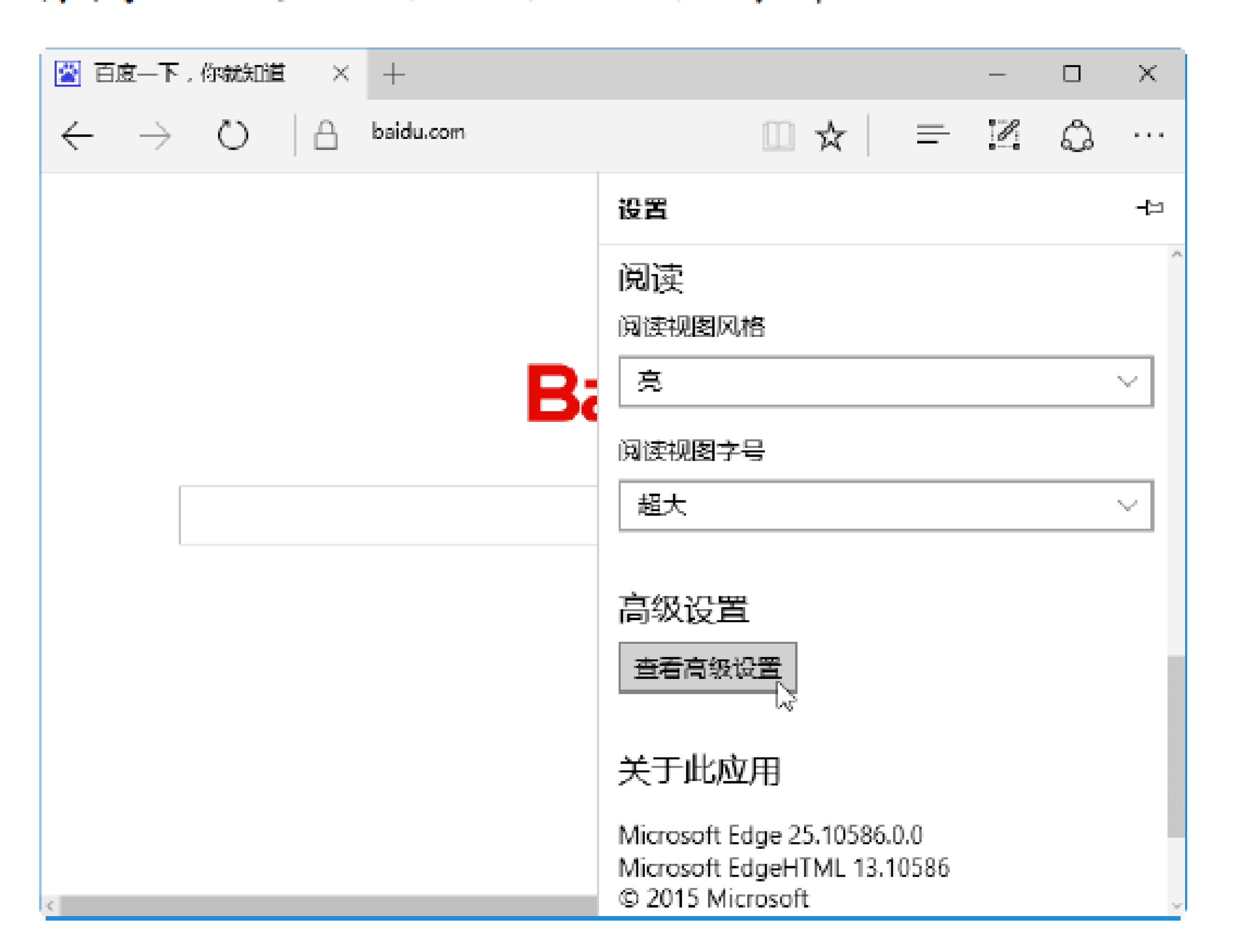
实战14：启用SmartScreen筛选功能

启用SmartScreen筛选功能，可以保护用户的计算机免受不良网站和下载内容的威胁。启用SmartScreen筛选功能的操作步骤如下。

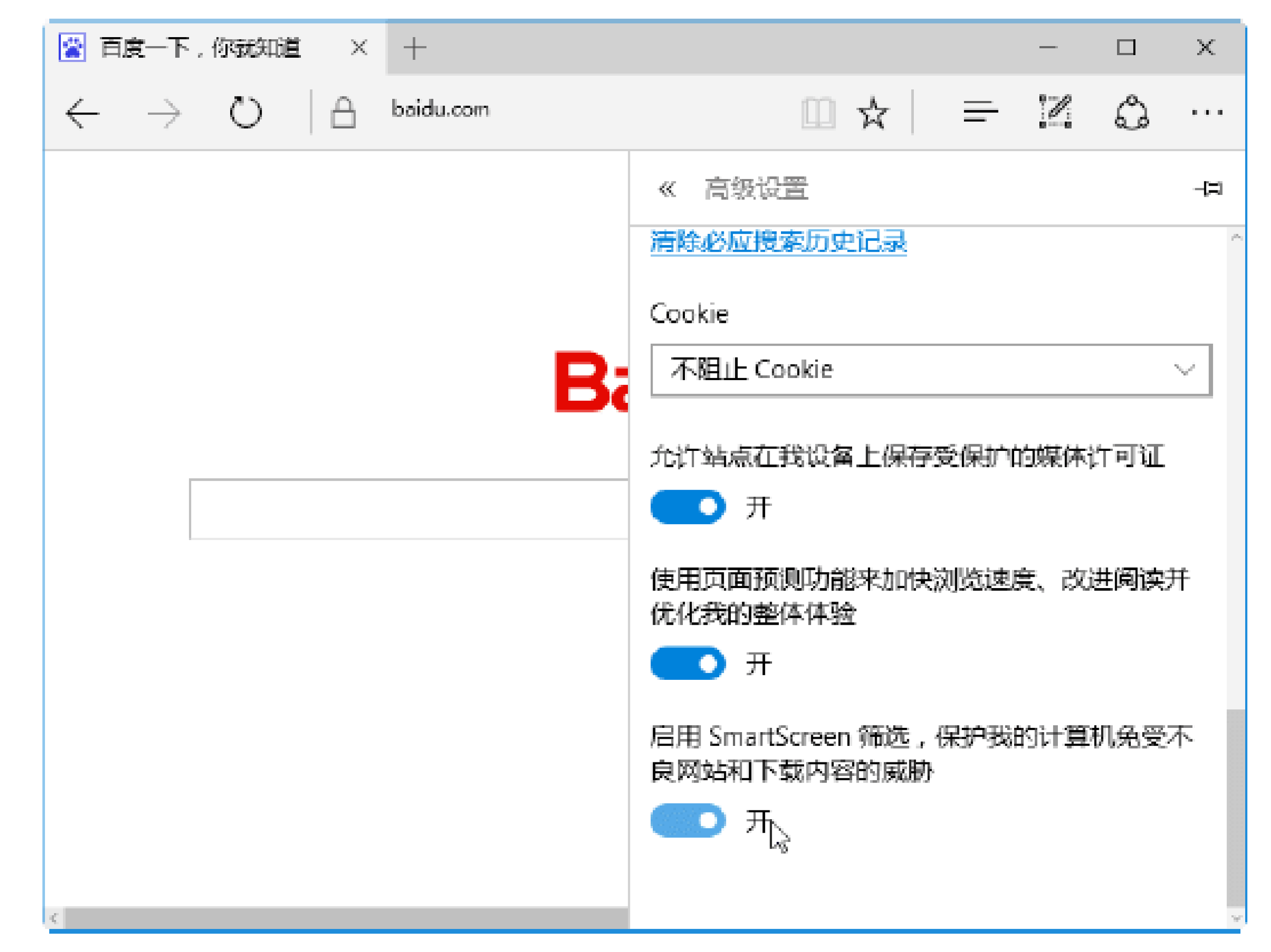
Step 01 打开Microsoft Edge浏览器，单击窗口中的“更多”按钮，在弹出的下拉列表中选择“设置”选项，如下图所示。



Step 02 打开“设置”界面，在其中单击“查看高级设置”按钮，如下图所示。



Step 03 打开“高级设置”工作界面，在其中将“启动SmartScreen筛选，保护我的计算机免受不良网站和下载内容的威胁”下方的“开/关”按钮设置为“开”，即可启用SmartScreen筛选功能，如下图所示。





8.4 使用工具保护浏览器的安全

除了可以利用网页浏览器自身的防护功能来保护网页浏览器的安全外，用户还可以借助第三方软件来保护网页浏览器。

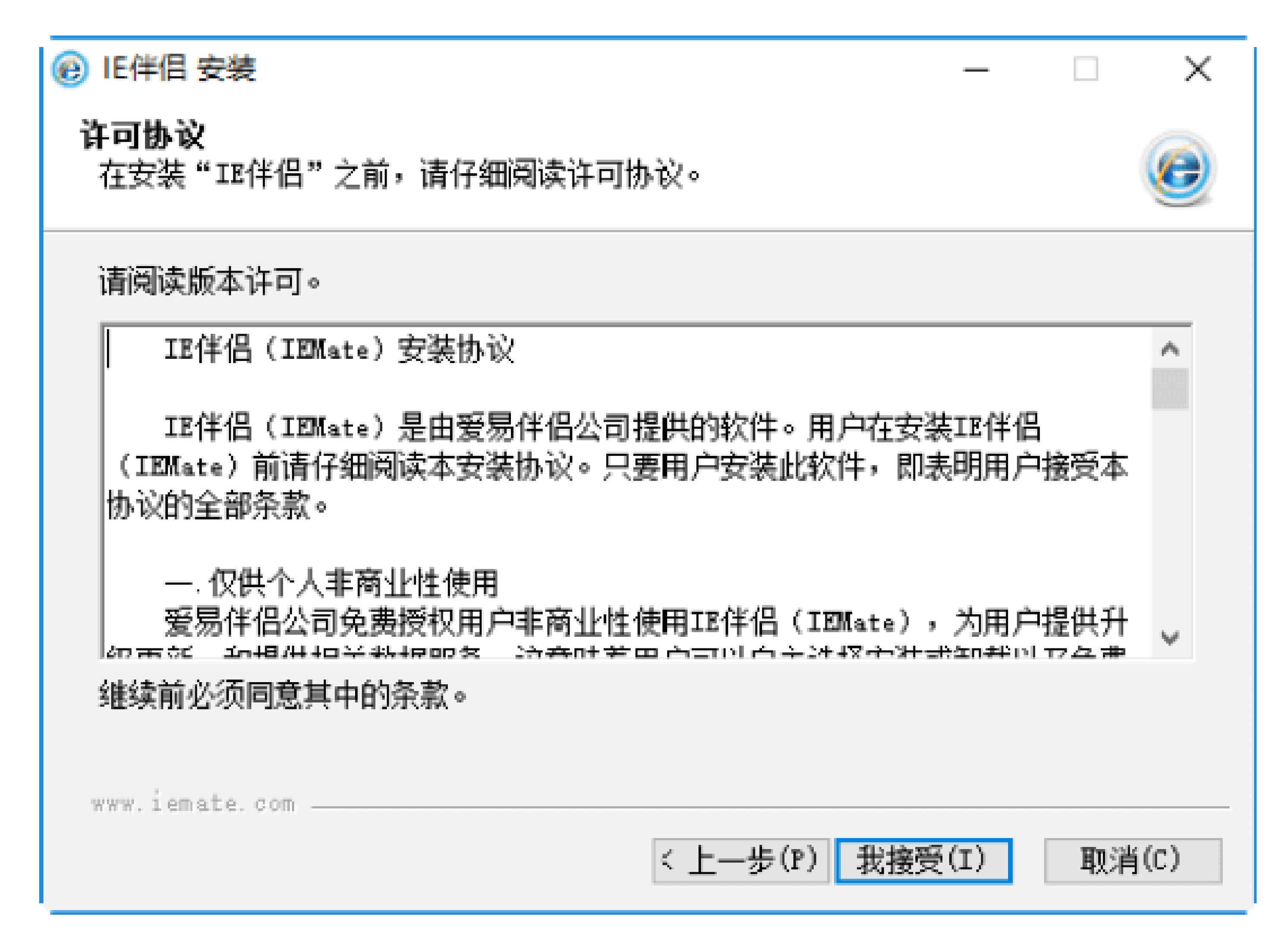
实战15：使用IE伴侣快速修复浏览器

IE伴侣（IEMate）是一款基于Internet Explorer的免费修复专家软件，从易用、安全、个性化角度通过IE修复优化浏览器性能。使用IE伴侣快速修复IE浏览器的具体操作步骤如下。

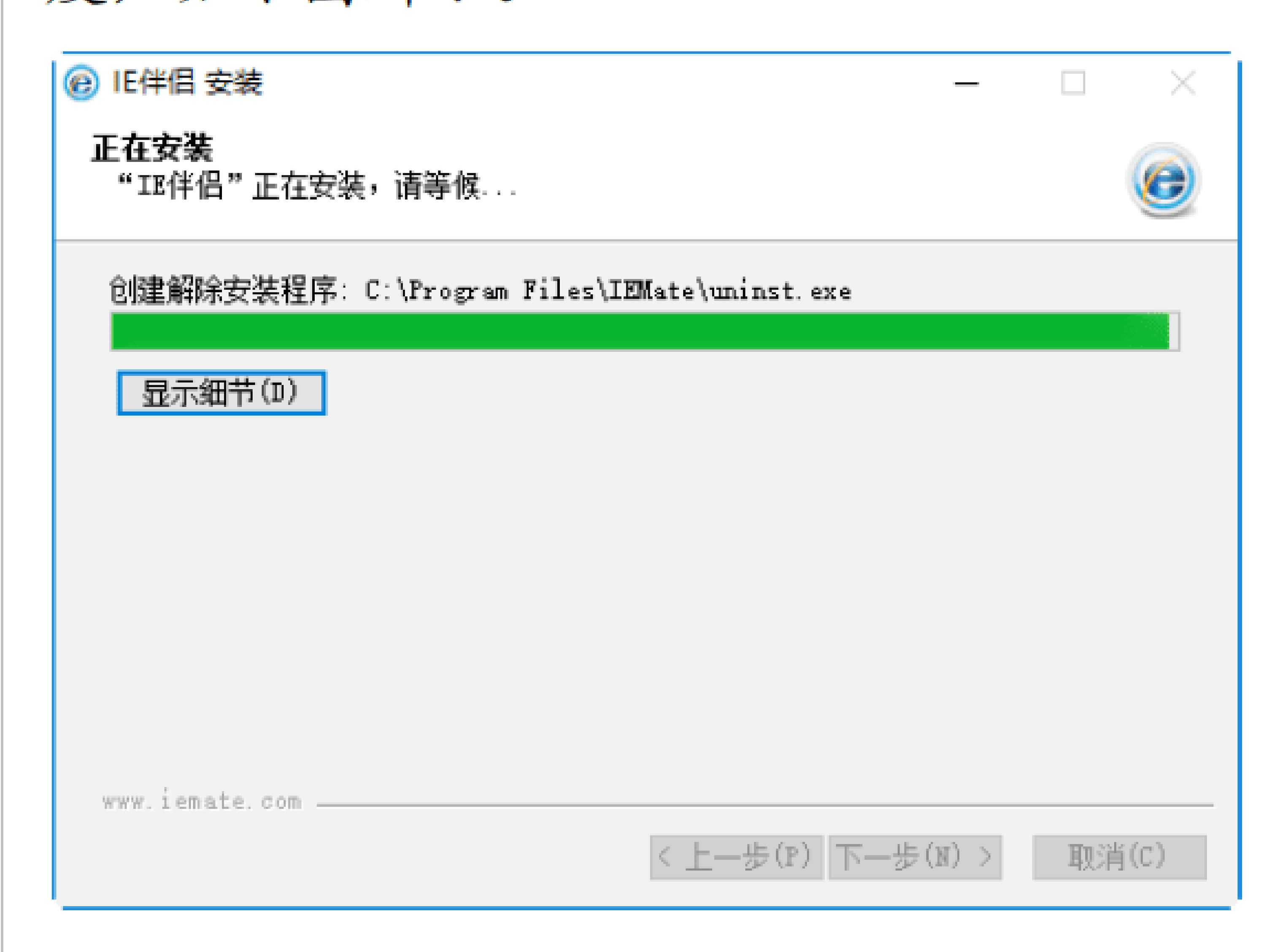
Step 01 双击下载IE伴侣（IEMate）安装程序，打开“欢迎使用IE伴侣安装向导”对话框，如下图所示。



Step 02 单击“下一步”按钮，进入“许可协议”对话框，用户在安装之前需要阅读相关的许可协议，如下图所示。



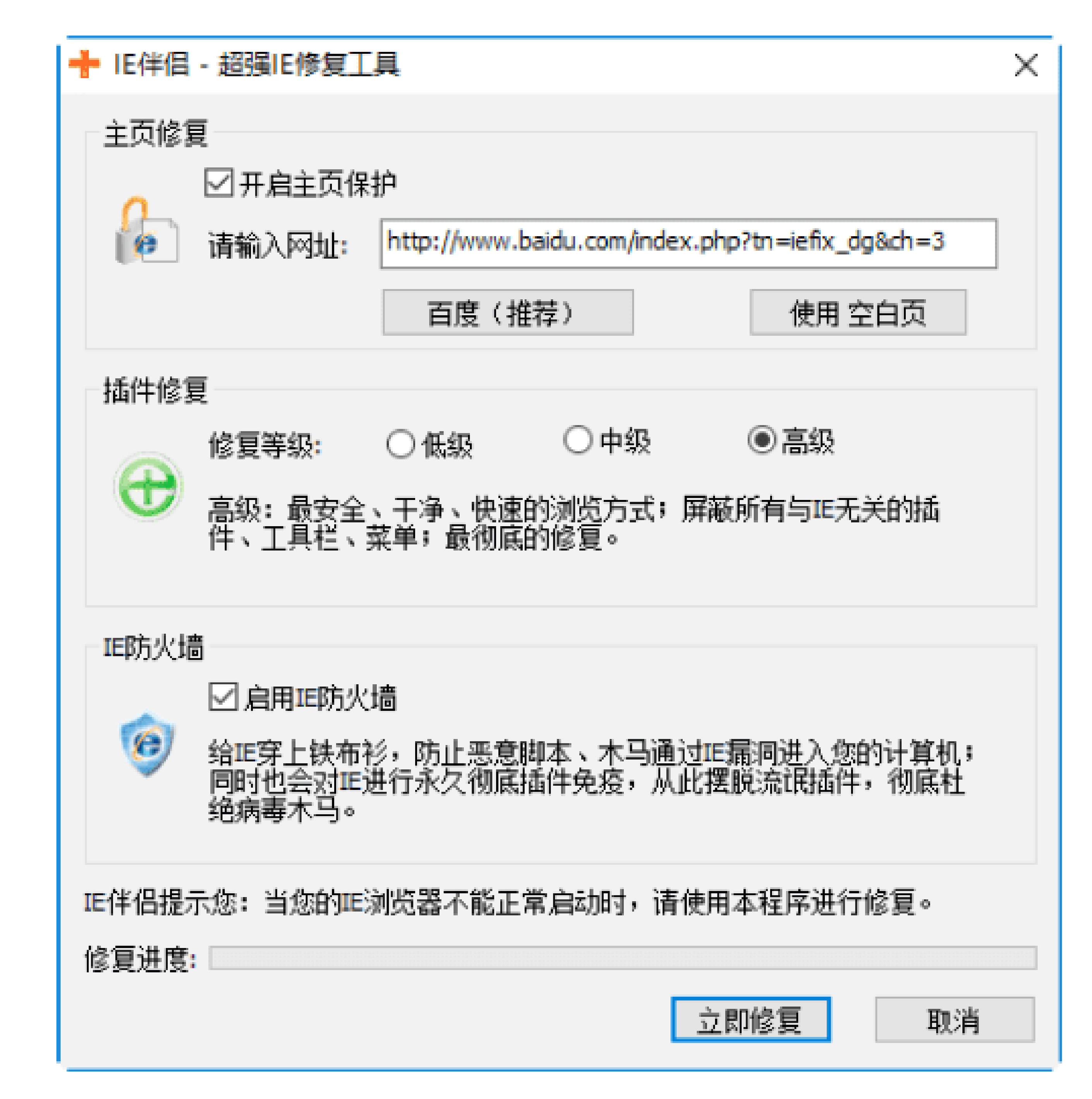
Step 03 单击“我接受”按钮，进入“正在安装”对话框，在其中显示程序安装的进度，如下图所示。



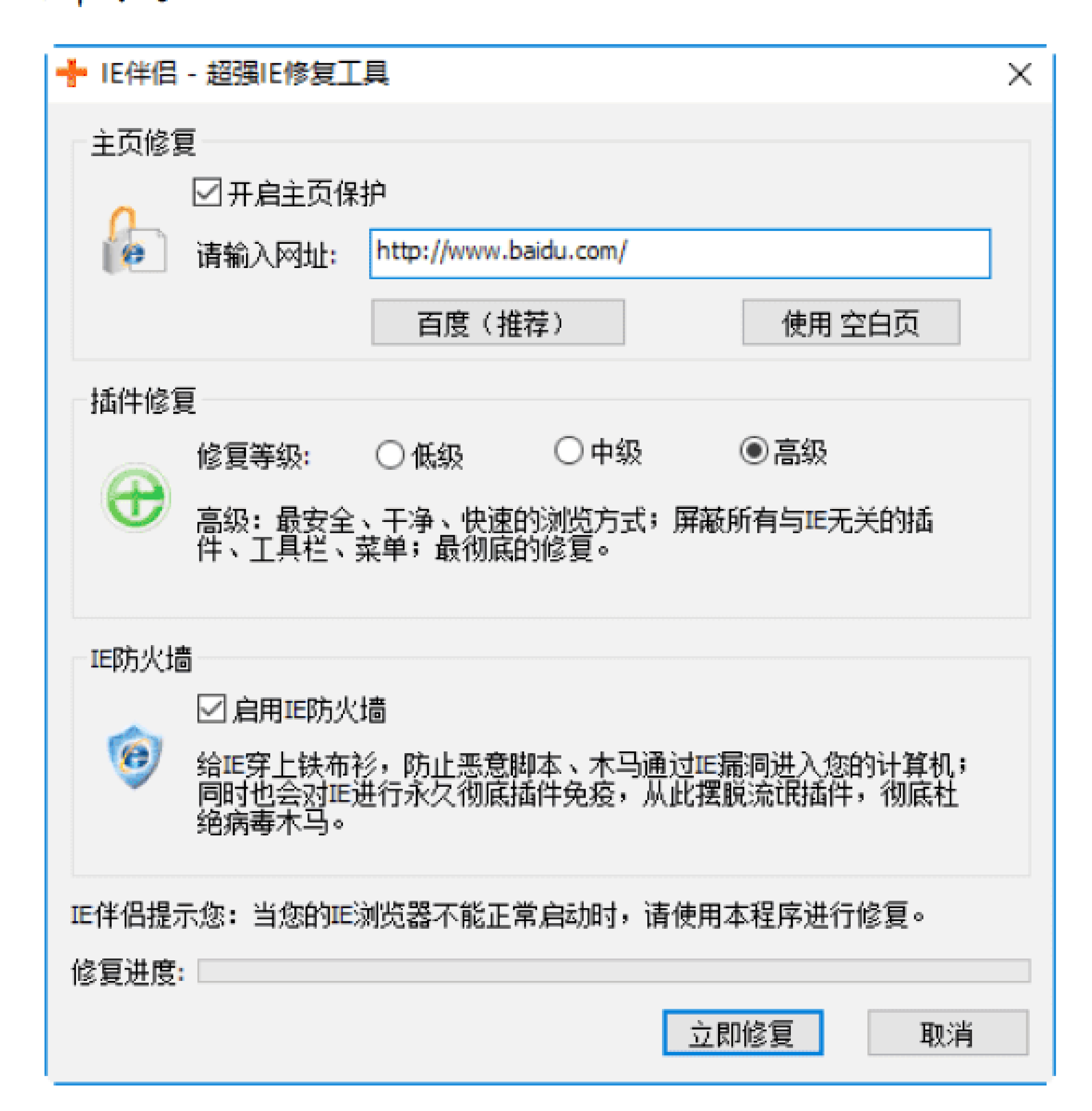
Step 04 安装完毕后，弹出“完成IE伴侣安装向导”对话框，在其中提示用户IE修复伴侣已经安装在系统之中了，勾选“运行IE紧急修复工具”复选框，如下图所示。



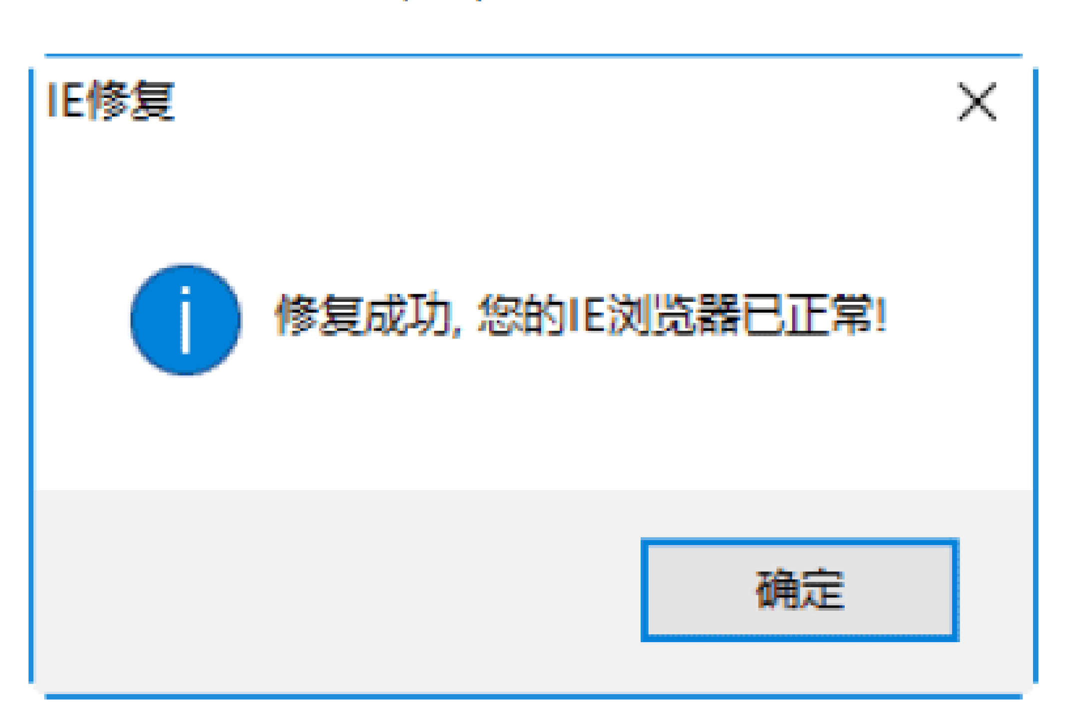
Step 05 单击“完成”按钮，即可打开“IE伴侣-超强IE修复工具”对话框，如下图所示。



Step 06 在“主页修复”设置区域中的“请输入网址”文本框中输入想要开始的主页，并勾选“开启主页保护”复选框，如下图所示。



Step 07 单击“立即修复”按钮，即可成功修复被篡改的IE主页，并弹出修复成功的信息提示框，如下图所示。



Step 08 单击“确定”按钮，即可关闭信息提示框，IE浏览器已经正常工作，如下图所示。



实战16：使用IE修复专家修复浏览器



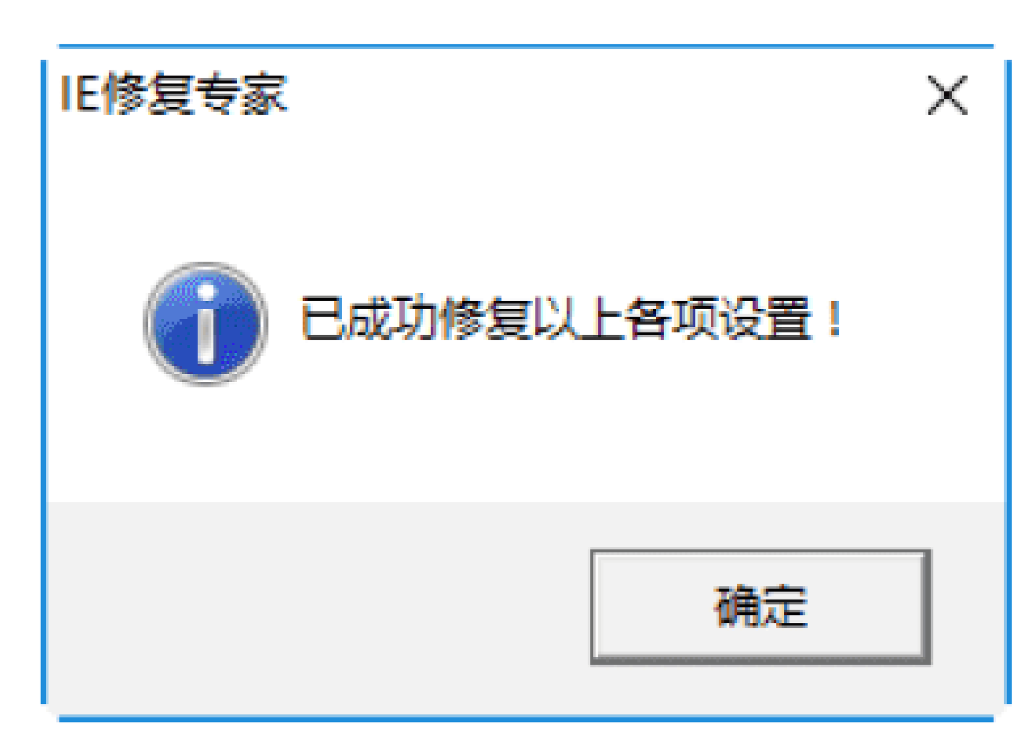
使用IE修复专家可以修复IE的标题栏、首页、右键菜单、工具栏按钮、工具栏菜单、附加工具栏、OutLook标题等；还可以全面修复各项Internet选项，包括常规、安全、连接、内容、高级等所有选项设置；并提供“一键修复”功能，单击即可自动修复所有设置。

使用IE修复专家修复IE浏览器的具体操作步骤如下。

Step 01 下载并安装IE修复专家后，打开“IE修复专家”主窗口，在其中选择“常规设置”选项，进入“常规设置”界面，在其中根据提示输入相应的内容，如下图所示。



Step 02 单击“常规修复”按钮，即可对IE浏览器进行常规修复，如下图所示。



Step 03 在“常规设置”界面中的“选项”设置区域中，用户还可以根据需要勾选相应的复选框，如下图所示。

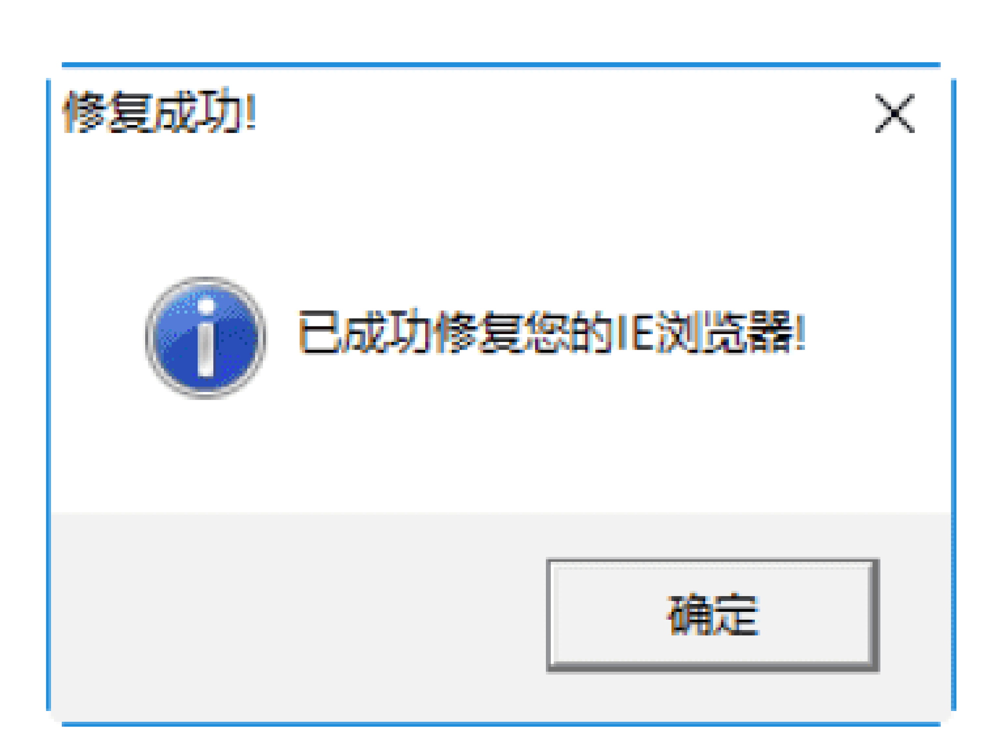




Step 04 单击“全面修复”按钮，打开“全面修复-修复选项设置”窗口，在其中勾选相应的修复选项，如下图所示。



Step 05 单击“立即修复”按钮，即可对IE浏览器进行全面修复，修复完毕后，弹出“修复成功”对话框，如下图所示。



8.5 实战演练

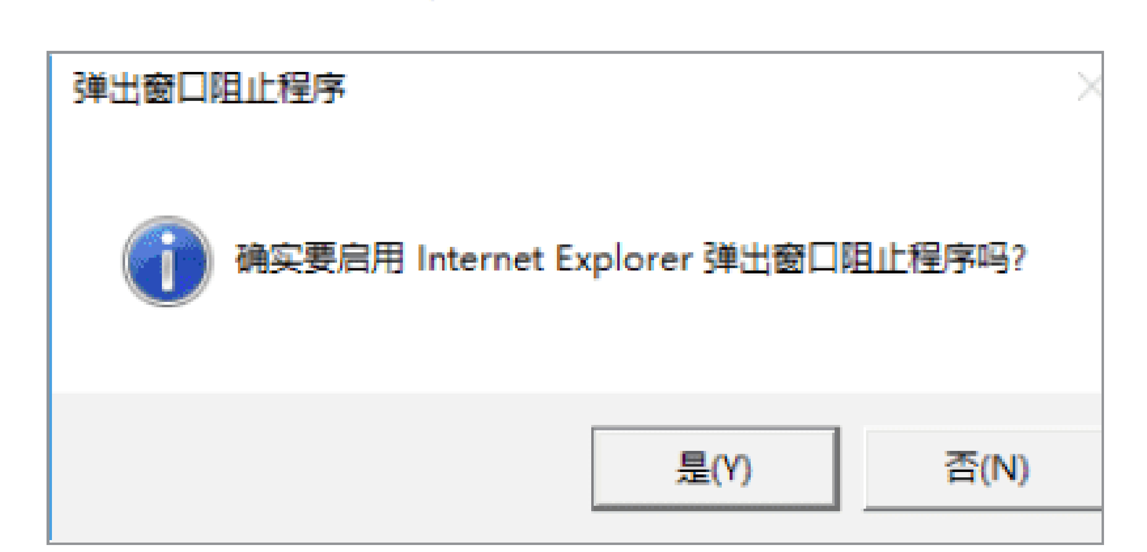
实战演练1——屏蔽浏览器网页广告弹窗

Internet Explorer 11浏览器具有屏蔽网页广告弹窗的功能，使用该功能屏蔽网页广告弹窗的操作步骤如下。

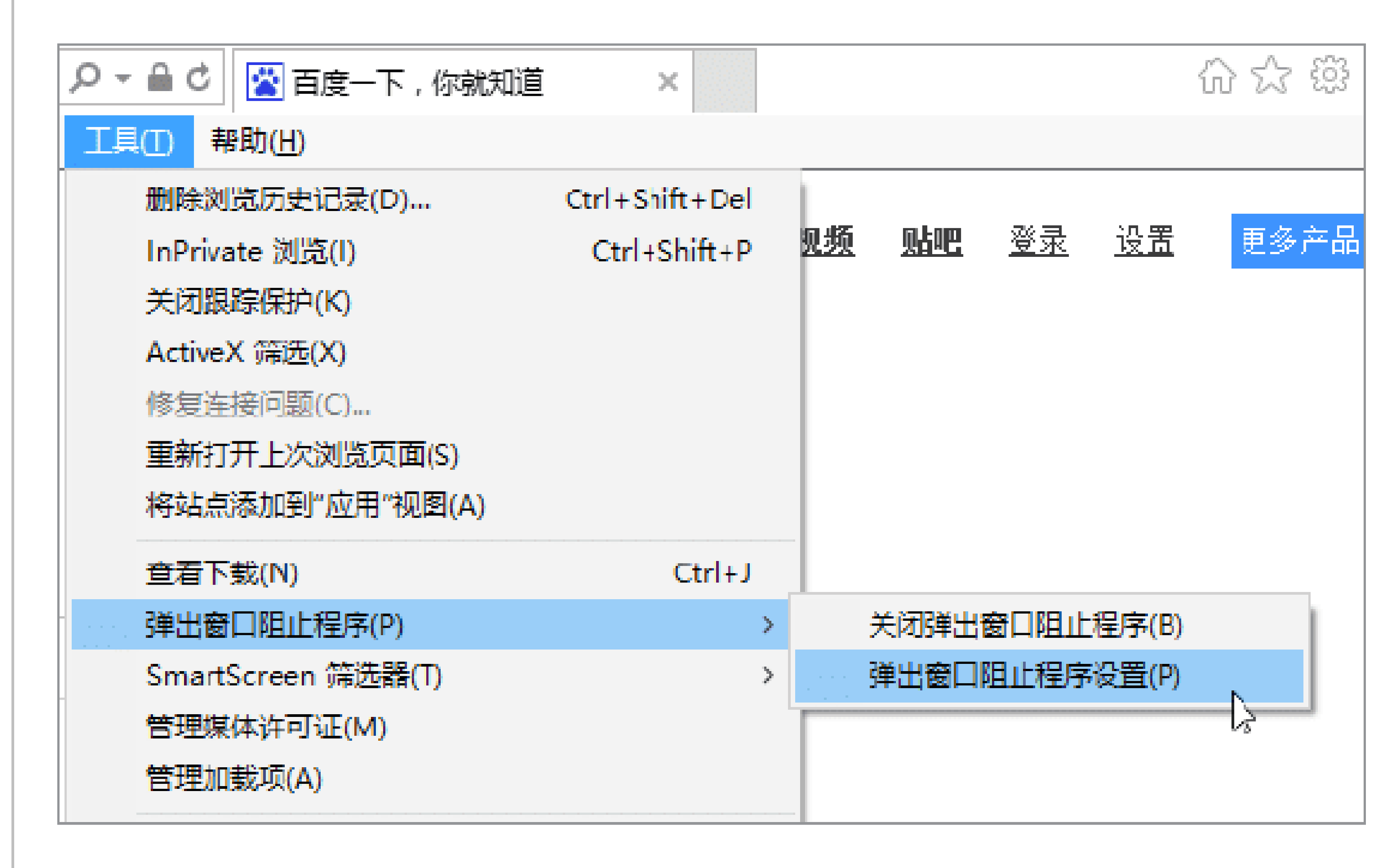
Step 01 在Internet Explorer 11浏览器的工作界面中选择“工具”→“弹出窗口阻止程序”→“启用弹出窗口阻止程序”选项，如下图所示。



Step 02 打开“弹出窗口阻止程序”对话框，提示用户是否确实要启用Internet Explorer弹出窗口阻止程序，如下图所示。

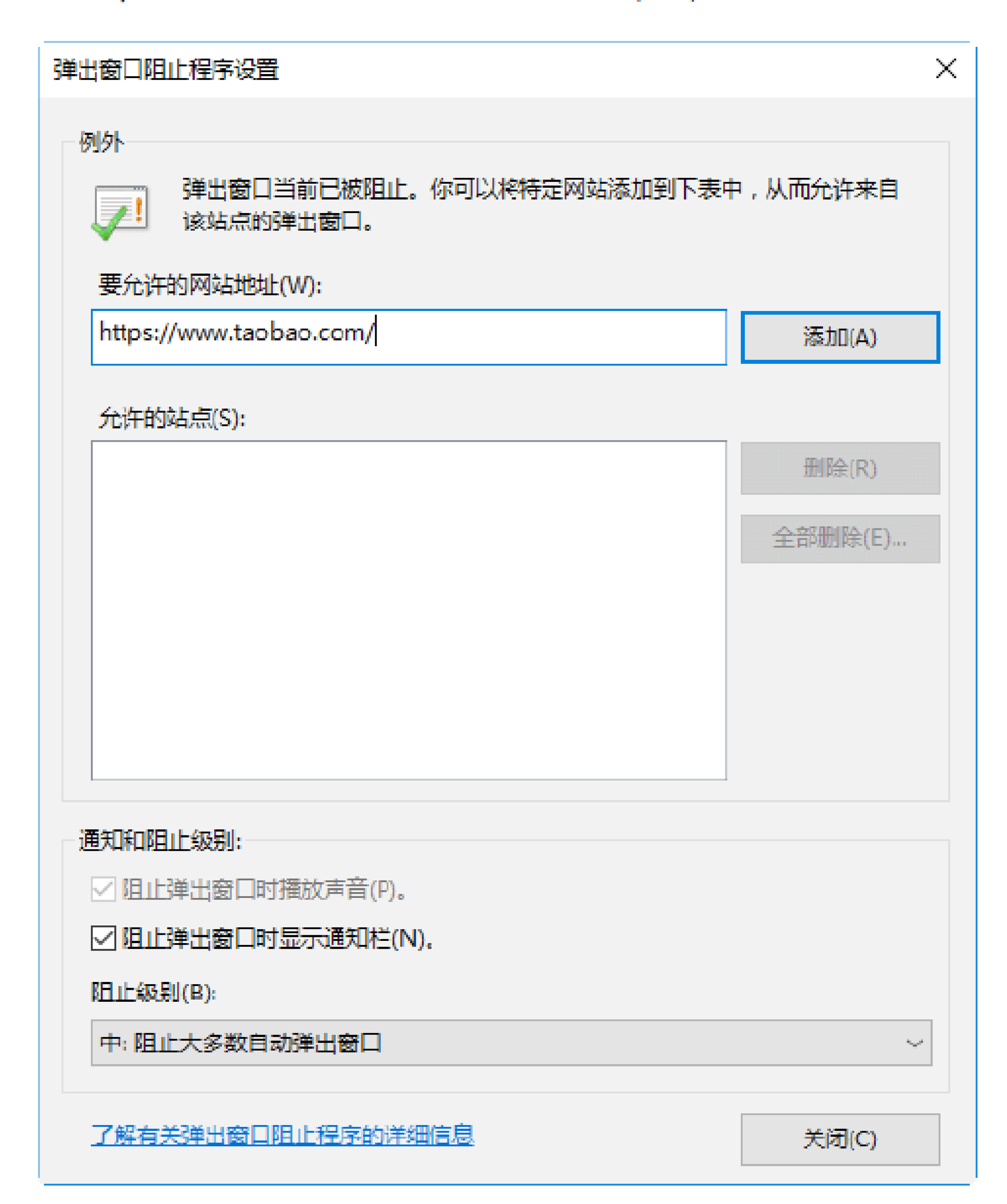


Step 03 单击“是”按钮，即可启用该功能，然后选择“工具”→“弹出窗口阻止程序”→“弹出窗口阻止程序设置”选项，如下图所示。

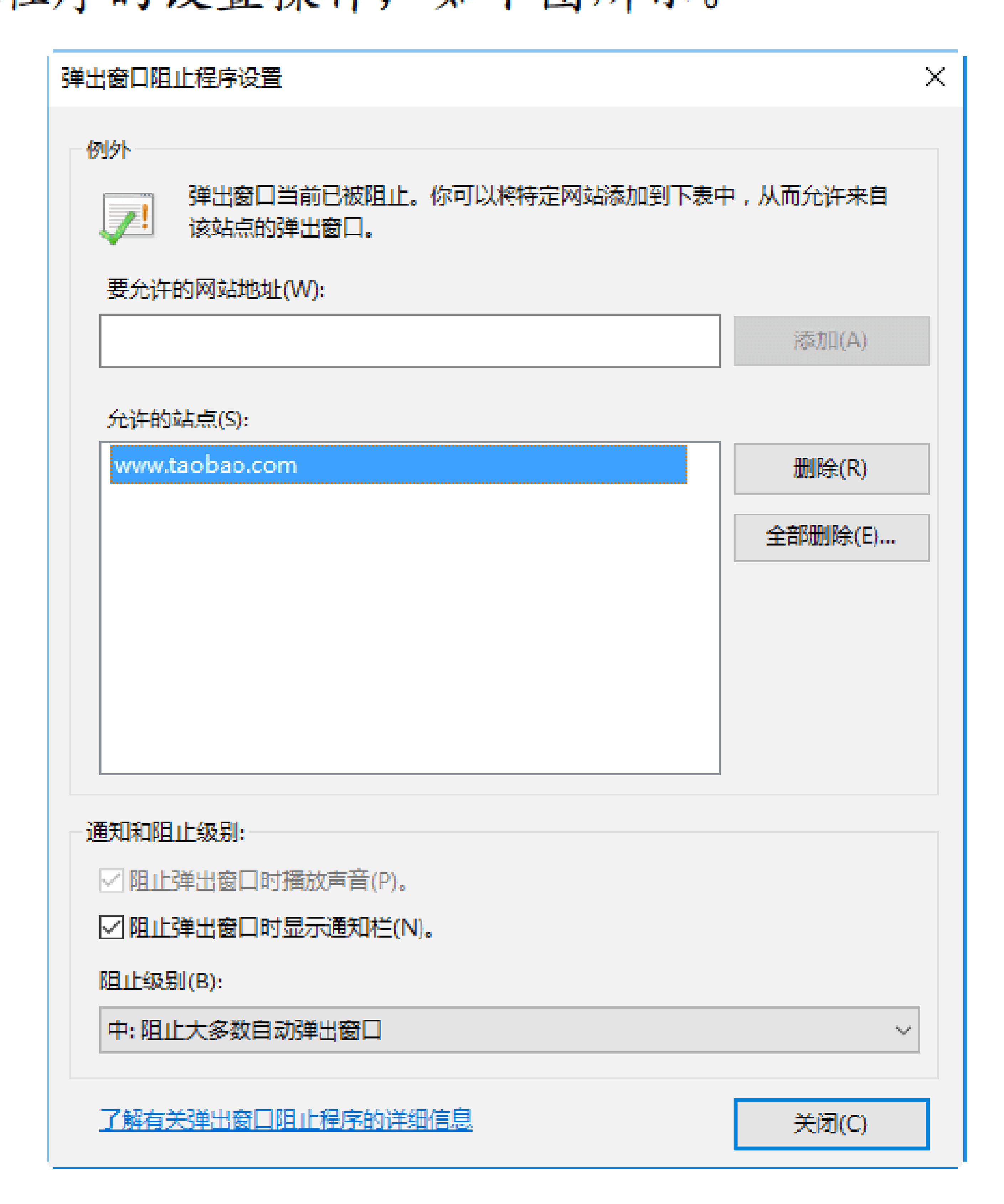


Step 04 打开“弹出窗口阻止程序设置”对话

框，在“要允许的网站地址”文本框中输入允许的网站地址，如下图所示。



Step 05 单击“添加”按钮，即可将输入的网站网址添加到“允许的站点”列表中。单击“关闭”按钮，即可完成弹出窗口阻止程序的设置操作，如下图所示。



实战演练2——将计算机收藏夹网址同步到手机

使用360安全浏览器可以将计算机收藏夹中的网址同步到手机中，其中360安全浏览器的版本要求在7.0以上。具体的操作步骤如下。

Step 01 在计算机中打开360安全浏览器8.1，如下图所示。



Step 02 单击工作界面左上角的浏览器标志，在弹出的界面中单击“登录账号”按钮，如下图所示。



Step 03 弹出“登录360账号”对话框，在其中输入账号与密码，如下图所示。





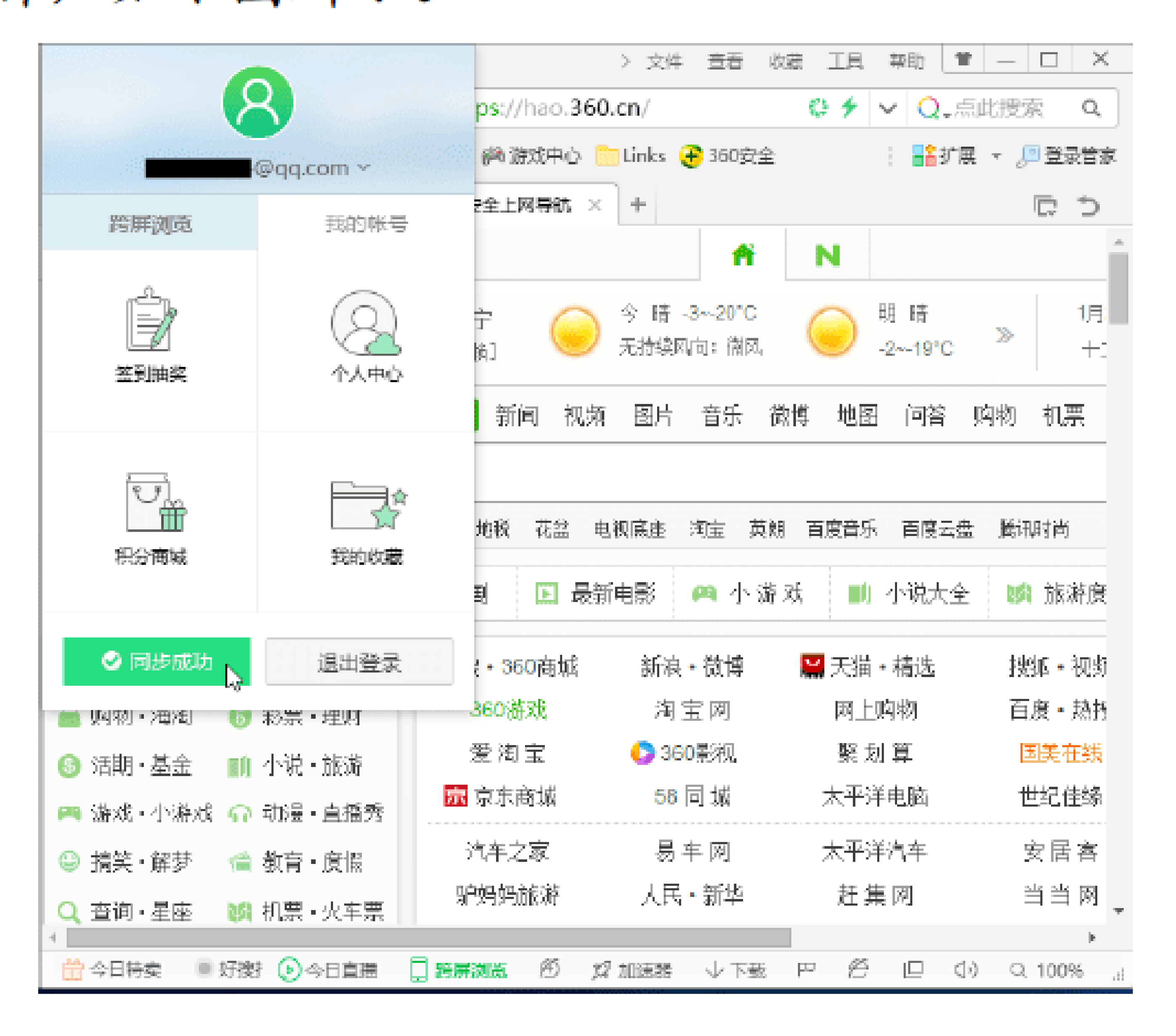
提示：如果没有账号，则可以单击“免费注册”按钮，在打开的界面中输入账号与密码，进行注册操作。



Step 04 输入完毕后，单击“登录”按钮，即可以会员的方式登录到360安全浏览器中，单击浏览器左上角的图标，在弹出的下拉列表中单击“手动同步”按钮，如下图所示。



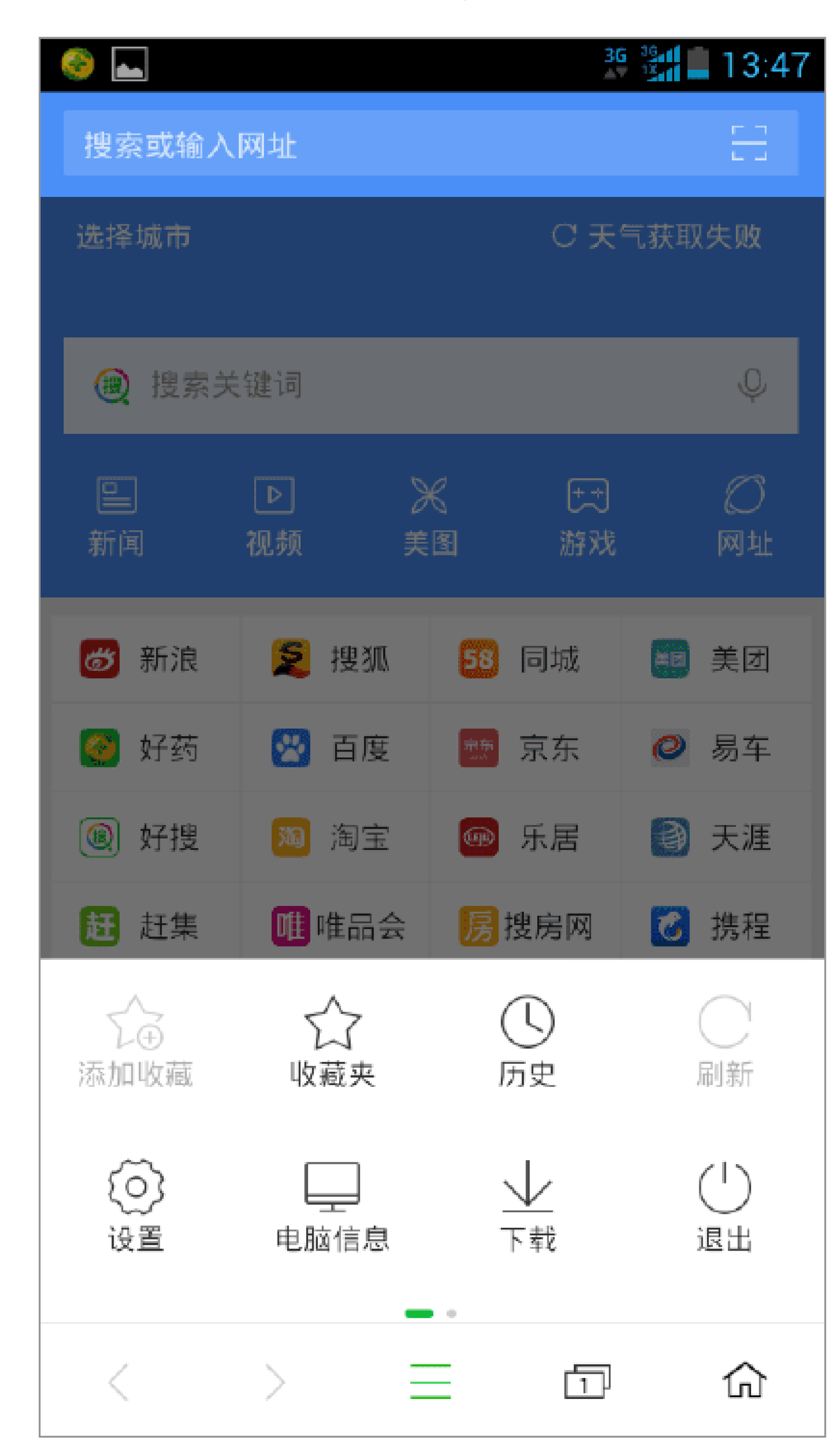
Step 05 即可将计算机中的收藏夹进行同步操作，如下图所示。



Step 06 进入手机操作环境，点按360手机浏览器图标，进入手机360浏览器工作界面，如下图所示。



Step 07 点按页面下方的“☰”按钮，打开手机360浏览器的设置界面，如下图所示。



Step 08 点按“收藏夹”图标，进入手机360浏览器的收藏夹界面，如下图所示。



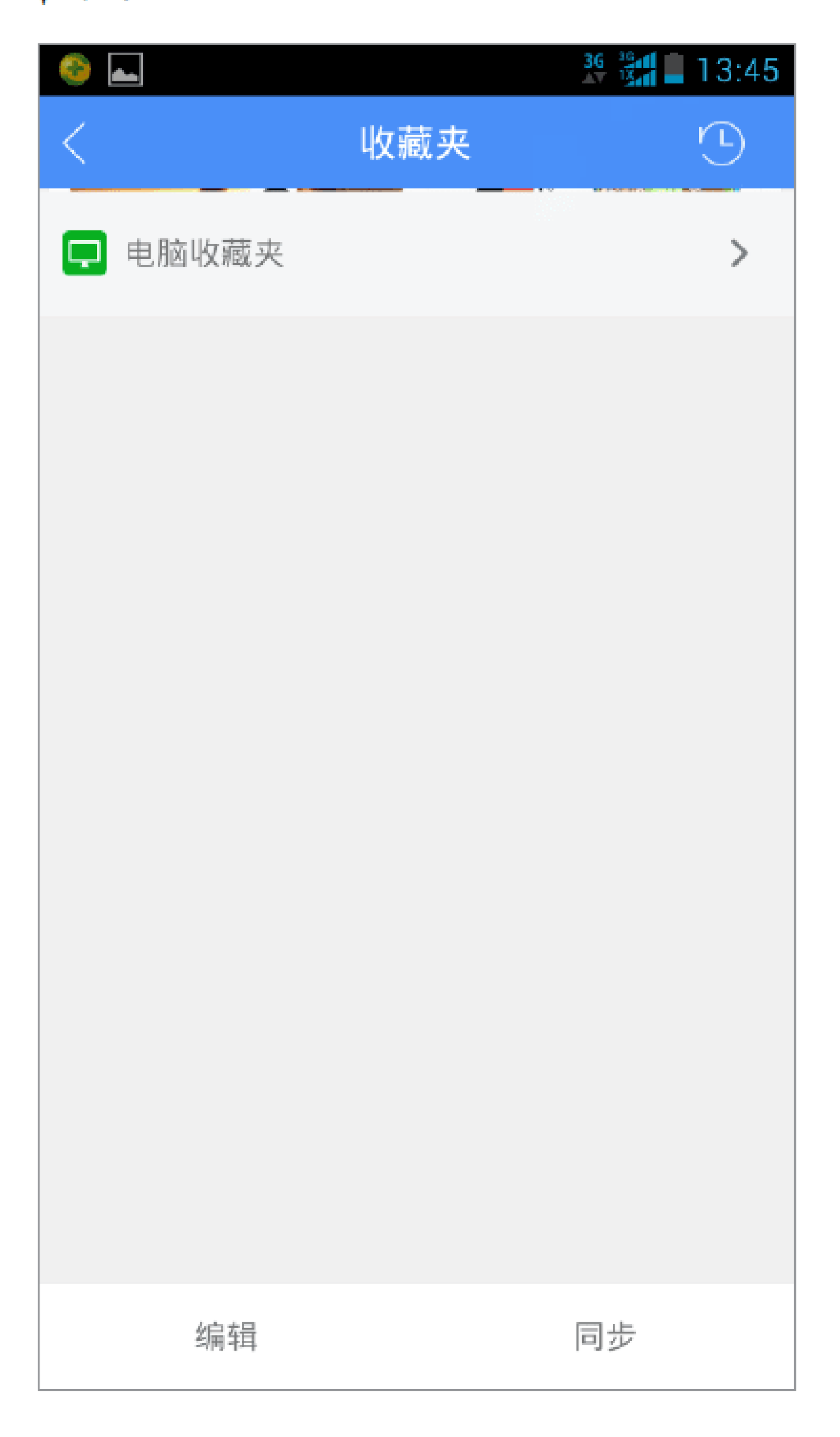
Step 09 点按“同步”按钮，打开“账号登录”界面，如下图所示。



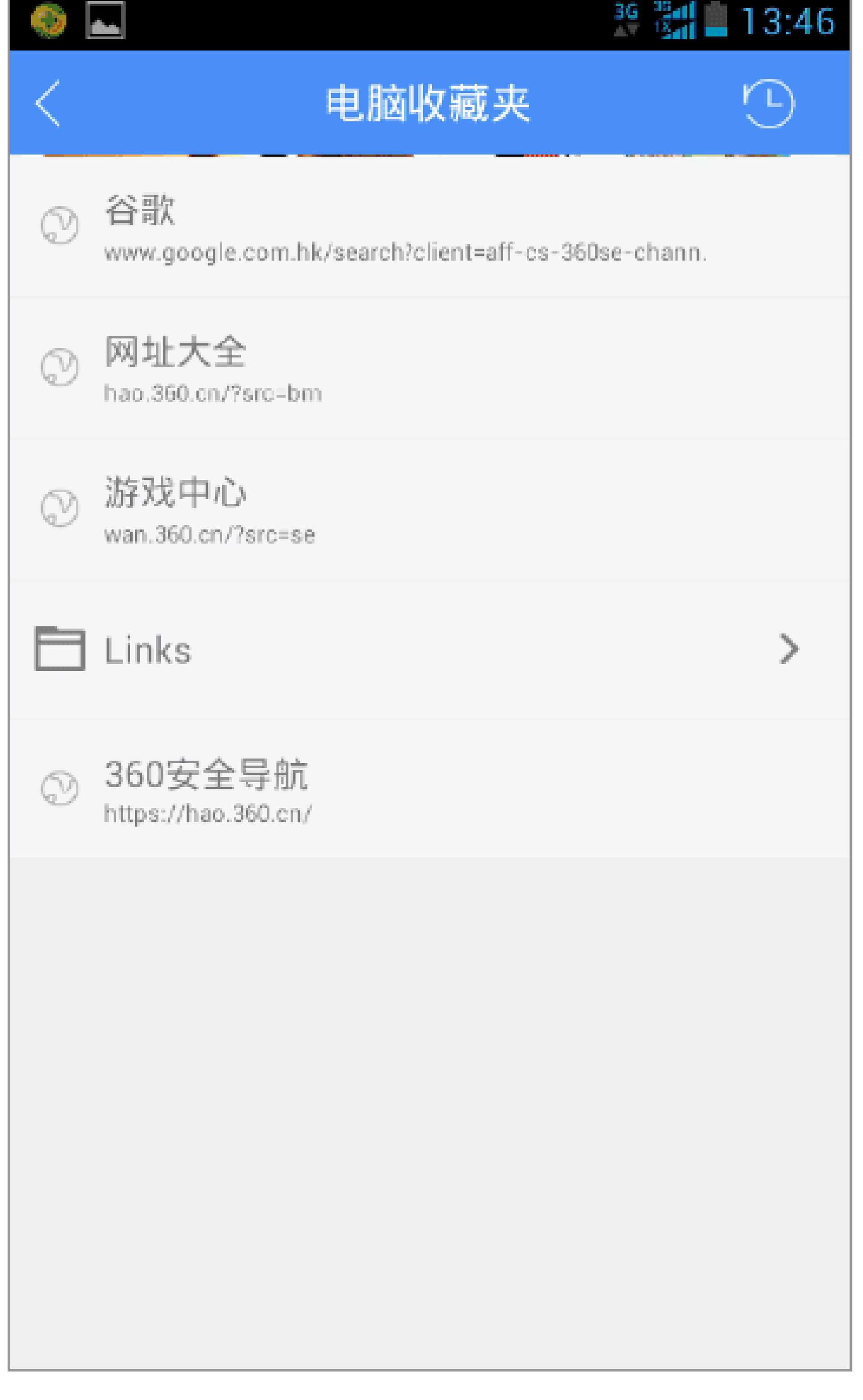
Step 10 在登录界面中输入账号与密码，这里需要注意的是手机登录的账号与密码与计算机登录的账户与密码必须一致，如下图所示。



Step 11 单击“立即登录”按钮，即可以会员的方式登录到手机360浏览器中，在打开的界面中可以看到“计算机收藏夹”选项，如下图所示。



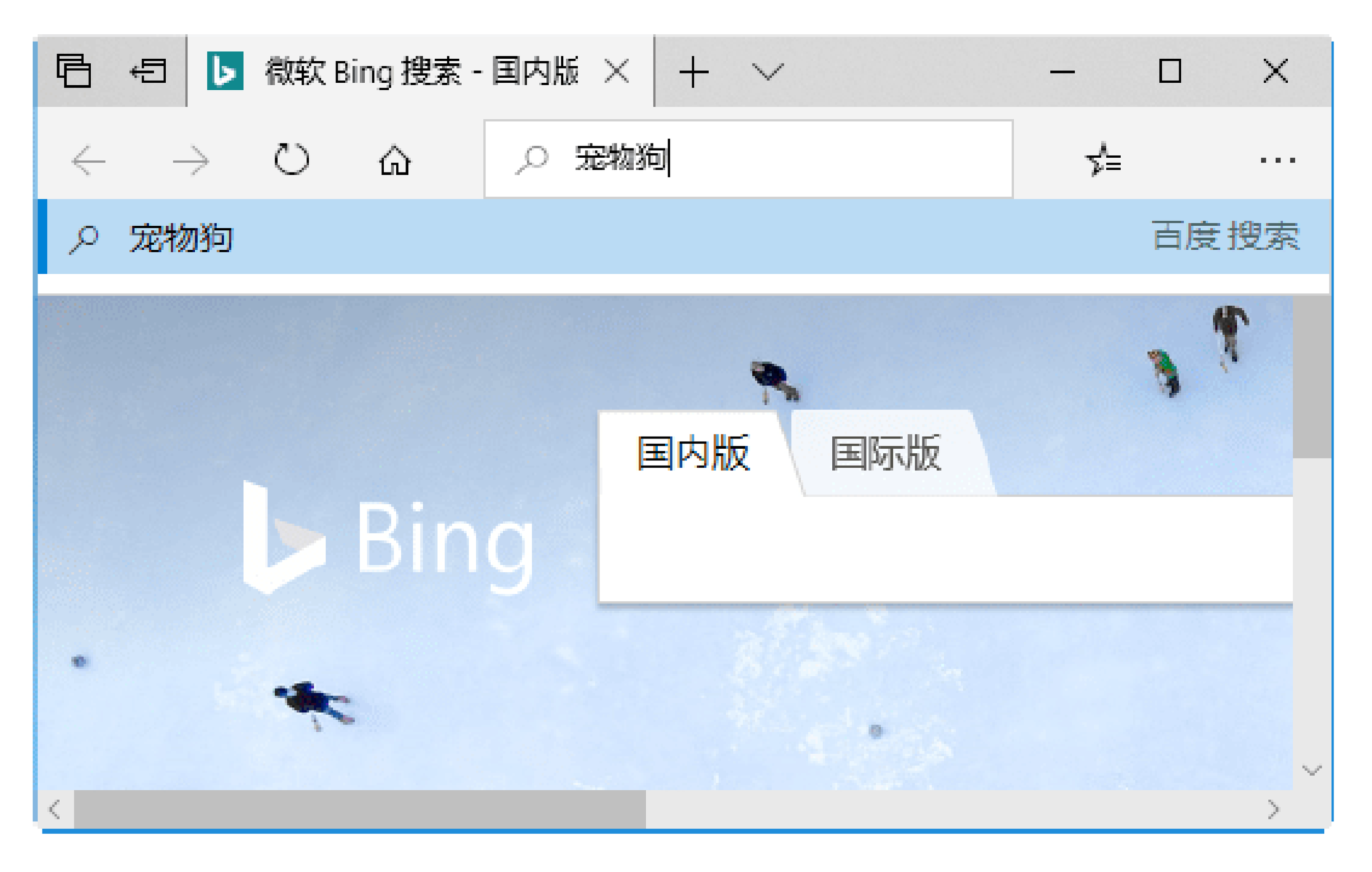
Step 12 点按“计算机收藏夹”选项，即可打开“计算机收藏夹”操作界面，在其中可以看到计算机中的收藏夹的网址信息出现在手机浏览器的收藏夹中，这就说明收藏夹同步完成，如下图所示。



8.6　小试身手

练习1：使用地址栏进行关键词搜索

在进行网络搜索时，不是只有打开搜索引擎网站，才能进行内容搜索，用户可以直接将关键词输入到浏览器的地址栏中，进行搜索查询，如在地址栏中输入“宠物狗”，如下图所示。



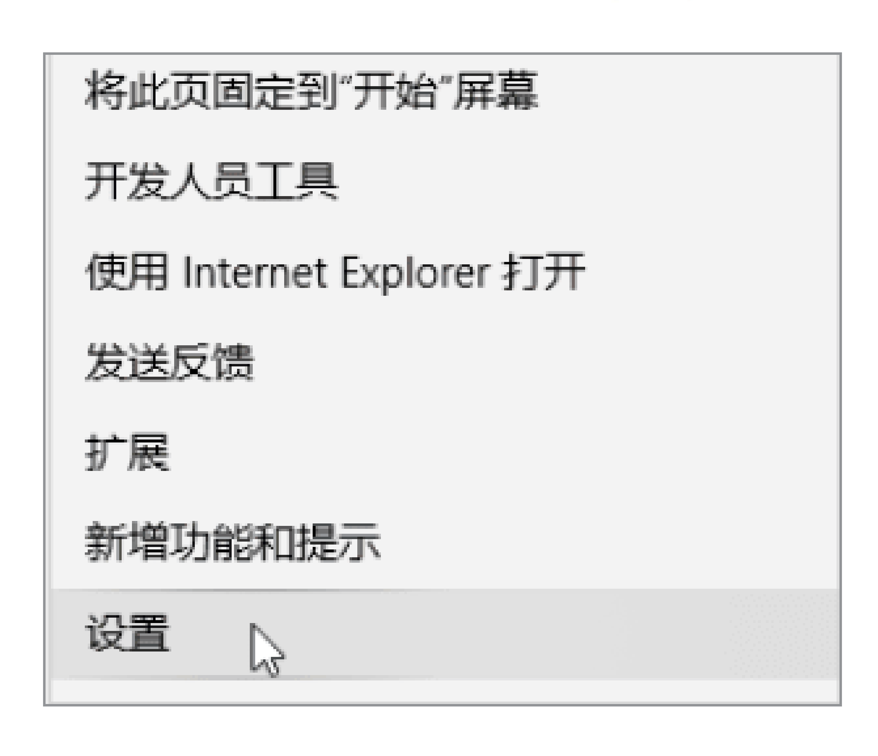
按Enter键，即可搜索出相关结果，如下图所示。



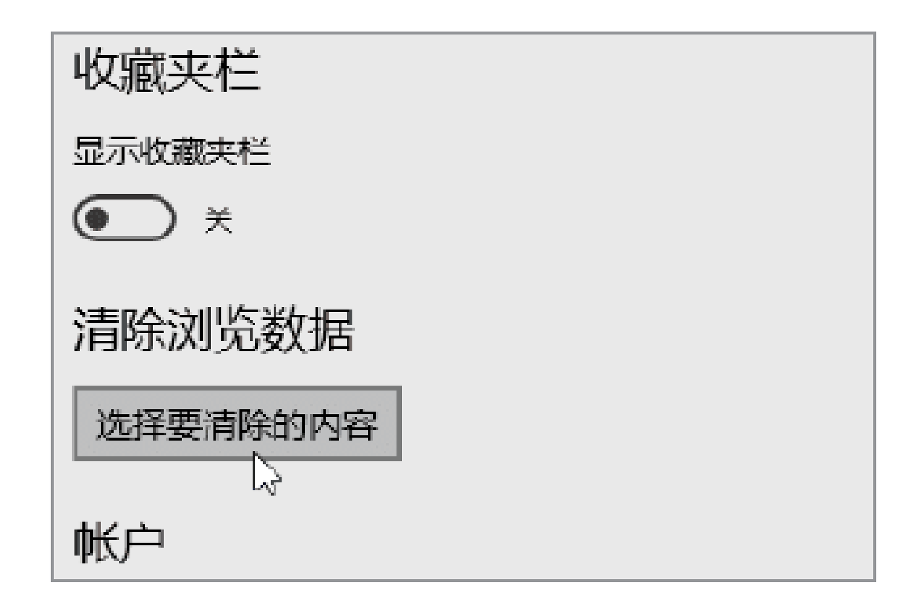
练习2：清除Microsoft Edge中的浏览数据

浏览器在上网时会保存很多的上网记录，这些上网记录不但随着时间的增加越来越多，而且还有可能泄露用户的隐私信息。如果不想让别人看见自己的上网记录，则可以把上网记录删除。具体的操作步骤如下。

Step 01 打开Microsoft Edge浏览器，单击右上角的“更多操作”按钮···，在弹出的列表中选择“设置”选项，如下图所示。

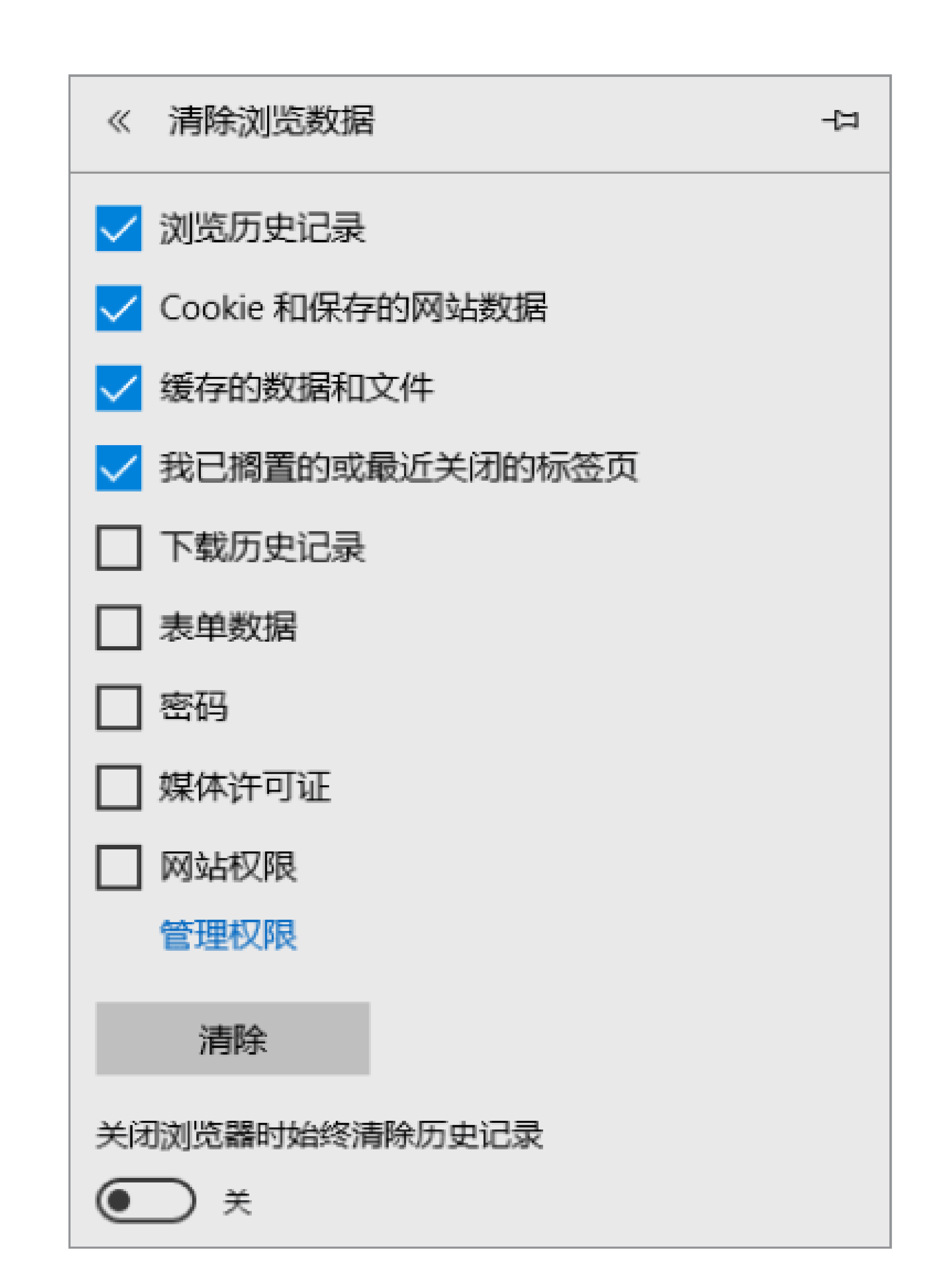


Step 02 打开“设置”窗格，单击“清除浏览数据”组下的“选择要清除的内容”按钮，如下图所示。

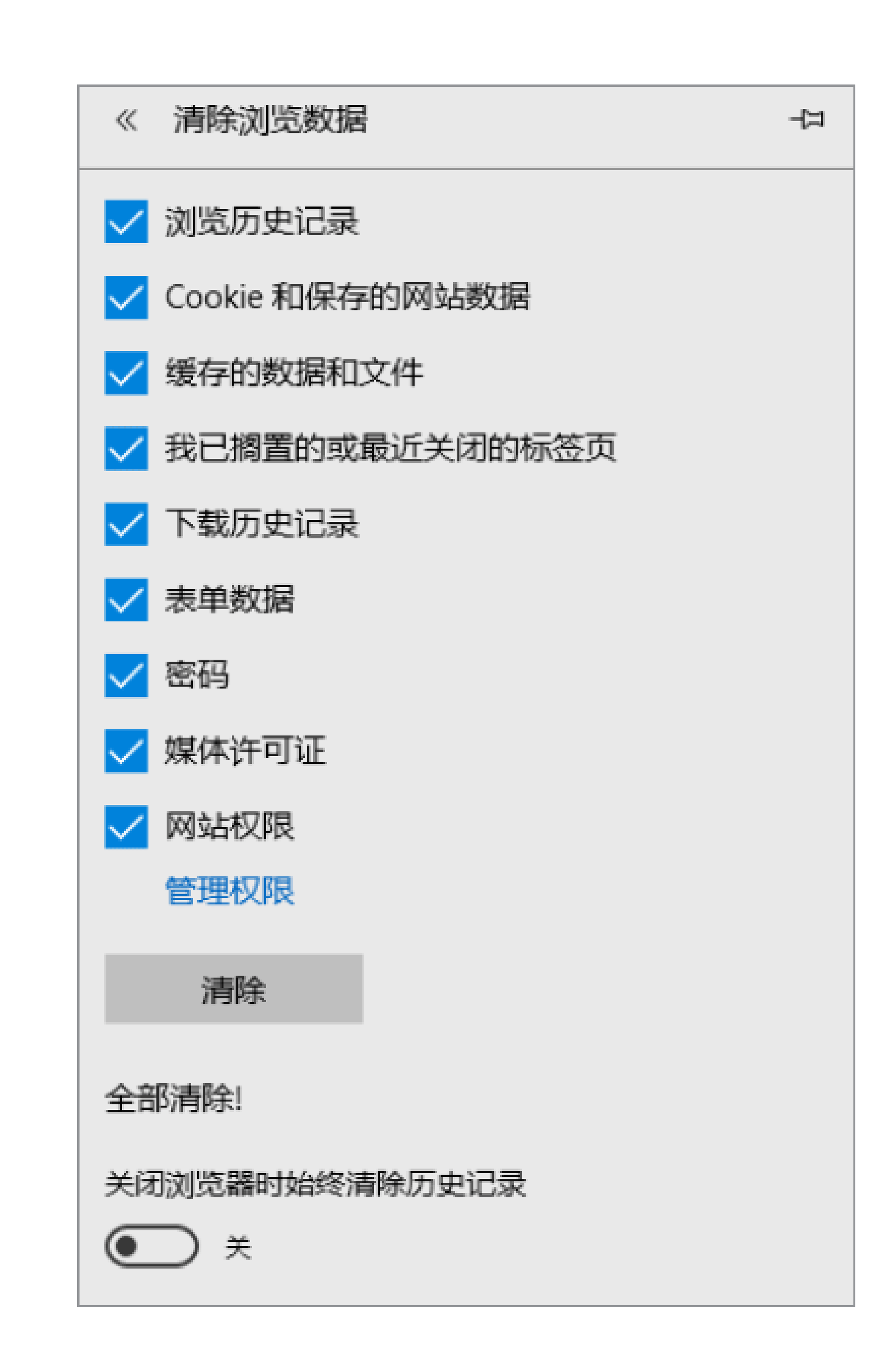


Step 03 弹出“清除浏览数据”窗格，单击选中要清除的浏览数据内容，单击“清除”按钮，如下图所示。





Step 04 开始清除浏览数据，清除完成后，即可看到历史纪录中所有的浏览记录都被清除，如下图所示。



第9章　有线局域网的安全防护

局域网作为计算机网络的一个重要成员已经被广泛应用于社会的各个领域。局域网联网非常灵活，两台计算机就可以连成一个局域网。局域网的安全是内部网络安全的关键，如何保证局域网的安全性成为网络安全研究的一个重点。本章介绍局域网的安全防护，主要内容包括局域网的安全介绍、查看局域网中的主机信息、局域网的安全防护等。

9.1　局域网的安全介绍

目前越来越多的企业建立自己的局域网，以实现企业信息资源共享或者在局域网上运行各类业务系统。随着企业局域网应用范围的扩大、保存和传输的关键数据增多，局域网的安全性问题显得日益突出。

9.1.1　局域网基础知识

人们日常接触到的办公网络都是局域网，目前各个企业、学校、政府机关等部门中的网络大部分都是局域网。局域网主要用在一个部门内部，常局限于一个建筑物之内。在企业内部利用局域网办公已成为其经营管理活动必不可少的一部分。

局域网（Local Area Network，LAN）是指在某一区域内由多台计算机组成的计算机组，一般是方圆几千米。局域网把个人计算机、工作站和服务器连在一起，在局域网中可以进行管理文件、共享应用软件、共享打印机、安排工作组内的日程、发送电子邮件和传真通信服务等操作。局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个公司内的数百台计算机组成。

由于距离较近，传输速率较快，范围为10～1000Mb/s。局域网常见的分类方法有以下几种：

（1）按采用的技术可分为不同的种类，如Ether Net（以太网）、FDDI、Token Ring（令牌环）等。

（2）按联网的主机间的关系可分为两类：对等网和C/S（客户/服务器）网。

（3）按使用的操作系统不同可分为许多种，如Windows 网和Novell 网。

（4）按使用的传输介质可分为细缆（同轴）网、双绞线网和光纤网等。

局域网最主要的特点是：网络为一个单位所拥有，且地理范围和站点数目均有限。局域网具有如下的一些主要优点。

（1）网内主机主要为个人计算机，是专门适用于微机的网络系统。

（2）覆盖范围较小，一般在几千米之内，适用于单位内部联网。

（3）传输速率高，误码率低，可采用较低廉的传输介质。

（4）系统扩展和使用方便，可共享昂贵的外部设备和软件、数据。

（5）可靠性较高，适于数据处理和办公自动化。

9.1.2　局域网安全隐患

随着人类社会生活对因特网需求的日益增长，网络安全逐渐成为因特网及各项网络服务和应用进一步发展的关键问题。网络使用户以最快的速度获取信息，但是非公开性信息的被盗用和破坏，是目前局域网面临的主要问题。

1. 局域网病毒

在局域网中，网络病毒除了具有可传播性、可执行性、破坏性、隐蔽性等计算

机病毒的共同特点外，还具有以下几个新特点：

（1）传染速度快。在局域网中，由于通过服务器连接每一台计算机，这不仅给病毒传播提供了有效的通道，而且病毒传播速度很快。在正常情况下，只要网络中有一台计算机存在病毒，在很短的时间内，将会导致局域网内计算机相互感染繁殖。

（2）对网络破坏程度大。如果局域网感染病毒，将直接影响到整个网络系统的工作，轻则降低速度，重则破坏服务器重要数据信息，甚至导致整个网络系统崩溃。

（3）病毒不易清除。清除局域网中的计算机病毒，要比清除单机病毒复杂得多。局域网中只要有一台计算机未能完全消除病毒，就可能使整个网络重新被病毒感染，即使刚刚完成清除工作的计算机，也很有可能立即被局域网中的另一台带病毒计算机所感染。

2. ARP攻击

ARP攻击主要存在于局域网中，对网络安全危害极大。ARP攻击就是通过伪造的IP地址和MAC地址，实现ARP欺骗，它可以在网络中产生大量的ARP通信数据，使网络系统传输发生阻塞。如果攻击者持续不断地发出伪造的ARP响应包，就能更改目标主机ARP缓存中的IP-MAC地址，造成网络遭受攻击或中断。

3. Ping洪水攻击

Windows 提供一个Ping程序，使用它可以测试网络是否连接。Ping洪水攻击也称为ICMP入侵，它是利用Windows系统的漏洞来入侵的。攻击的原理是局域网中的客户机不断地向服务器发送大量的数据请求，这样服务器会因CPU使用率居高不下而崩溃。这种攻击方式也称DoS攻击（拒绝服务攻击），即在一个时段内连续向服务器发出大量请求，使服务器来不及回应而死机。

4. 嗅探

局域网是黑客进行监听嗅探的主要场所。黑客在局域网内的一个主机、网关上安装监听程序，就可以监听出整个局域域网的网络状态、数据流动、传输数据等信息。因为一般情况下，用户的所有信息，如账号和密码，都是以明文的形式在网络上传输的。目前可以在局域网中进行嗅探的工具很多，如Sniffer等。

9.2　查看局域网中的主机信息

通过查看局域网中的主机信息，可以掌握局域网中主机的运行情况，从而分析局域网是否受到攻击。利用专门的局域网查看工具可以查看局域网中各个主机的信息。

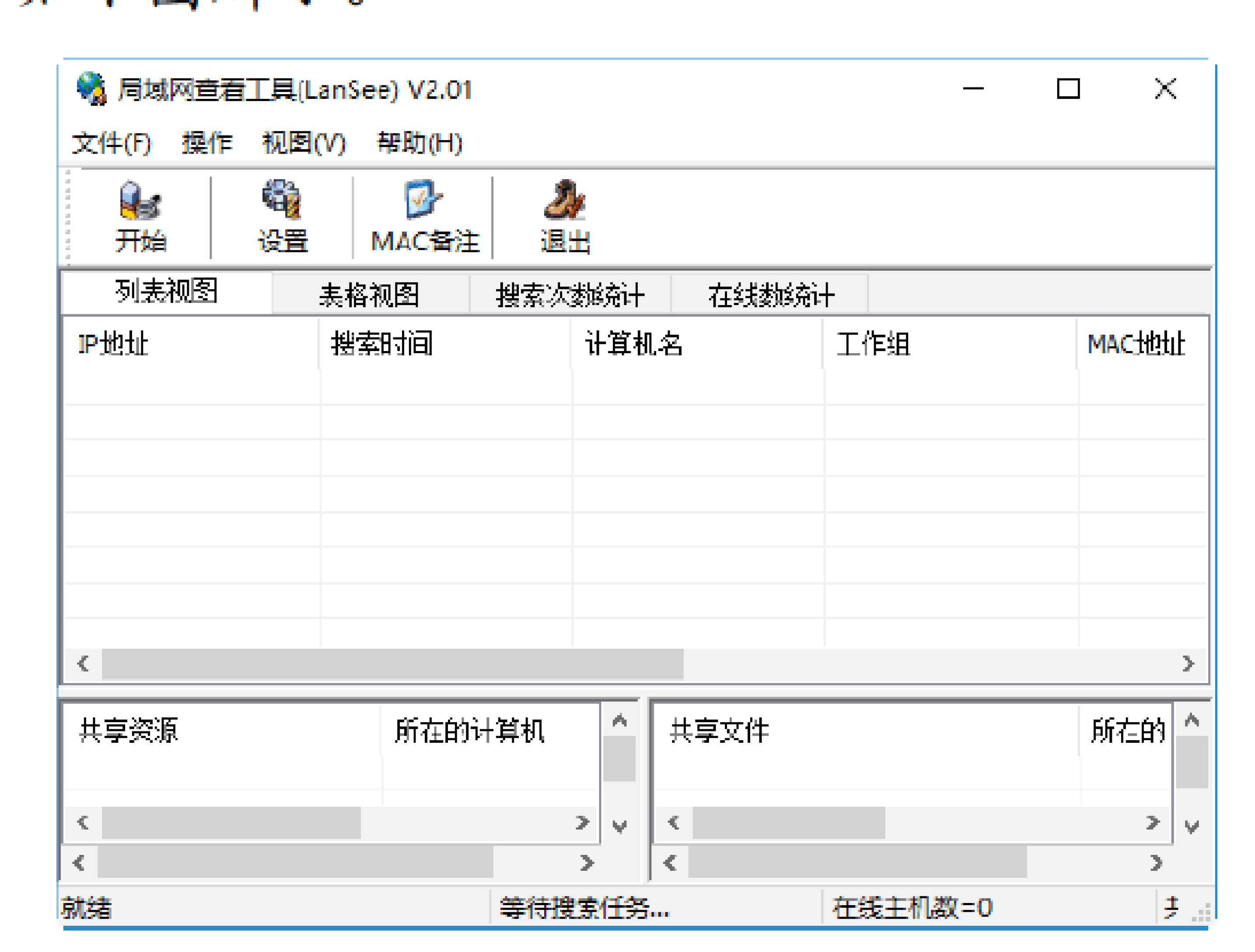
实战1：使用LanSee查看



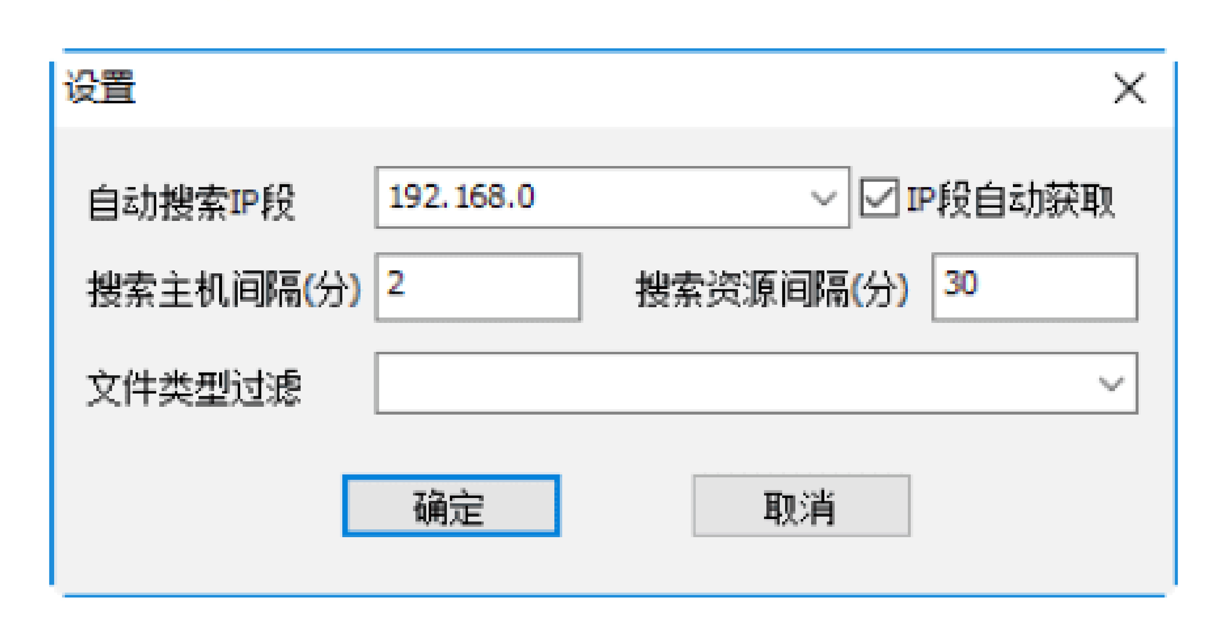
LanSee是一款对局域网上各种信息进行查看的工具。使用该工具可以快速搜索出局域网中的主机信息，如主机名、IP地址、MAC地址等；也可以搜索局域网中的共享资源与共享文件；还可以捕获各种数据包（TCP、UDP、ICMP、ARP），甚至可以从流过网卡的数据中嗅探出QQ号码、音乐、视频、图片等文件。

使用LanSee工具查看局域网中各种信息的具体操作步骤如下。

Step 01 双击下载的“局域网查看工具”程序，即可打开“局域网查看工具”主窗口，如下图所示。



Step 02 在工具栏单击“设置”按钮，即可打开“设置”对话框，在其中设置扫描计算机的相关参数，如下图所示。



Step 03 在“局域网查看工具”主窗口中单击“开始”按钮，即可搜索出指定IP段内的主机，在其中可看到各个主机的IP地址、计算机名、工作组、MAC地址等属性，如下图所示。

局域网查看工具(LanSee) V2.01

文件(F) 操作 视图(V) 帮助(H)

开始 设置 MAC备注 退出

列表视图 表格视图 搜索次数统计 在线数统计

IP地址	搜索时间	计算机名	工作组	MAC地址
192.168.0.107	2019-01-26 14:14:45	DESKTOP-5CVBNGI	WORKGROUP	00.23.24.D9.B6.E5
192.168.0.123	2019-01-26 14:14:46	XINHUNO7YDZVSSI	XINHUNO7YDZVSSI	58.FB.84.FB.58.10
192.168.0.143	2019-01-26 14:14:49	SC-201811151232	WORKGROUP	00.25.22.F9.5F.44
192.168.0.135	2019-01-26 14:14:50			98.54.1B.37.16.1C
192.168.0.1	2019-01-26 14:15:03			F4.83.CD.33.60.73

共享资源 所在的计算机 共享文件 所在的目录

就绪 等待搜索任务... 在线主机数=5 共享资源数

Step 04 如果想与某个主机建立连接，在搜索到的主机列表中右击该主机，在弹出的快捷菜单中选择“打开计算机”选项，即可打开“Windows安全”对话框，在其中输入该主机的用户名和密码，如下图所示。

Windows 安全

输入网络凭据

输入你的凭据以连接到:192.168.0.135

用户名

密码

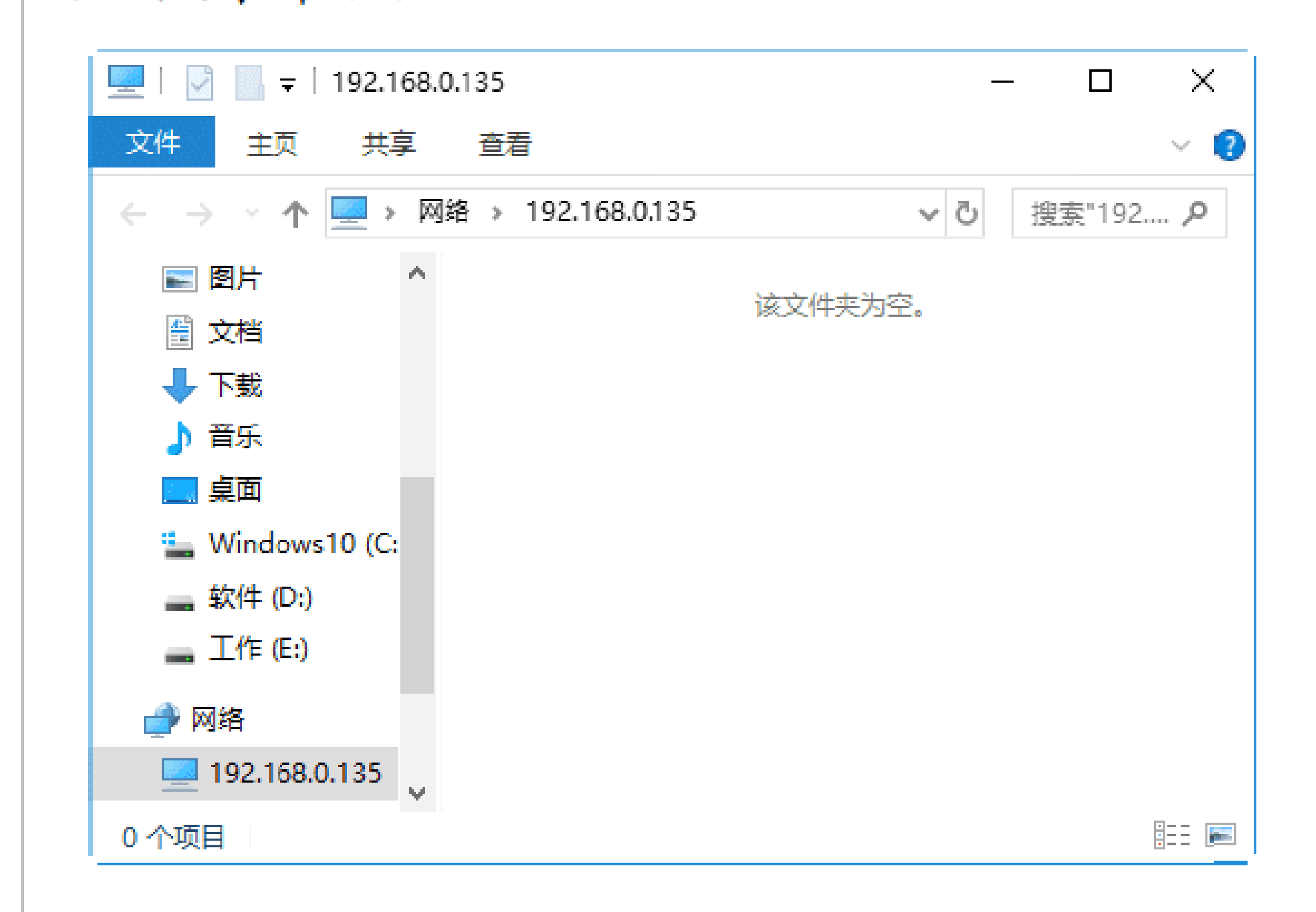
域: DESKTOP-67NQBIF

记住我的凭据

用户名或密码不正确。

确定 取消

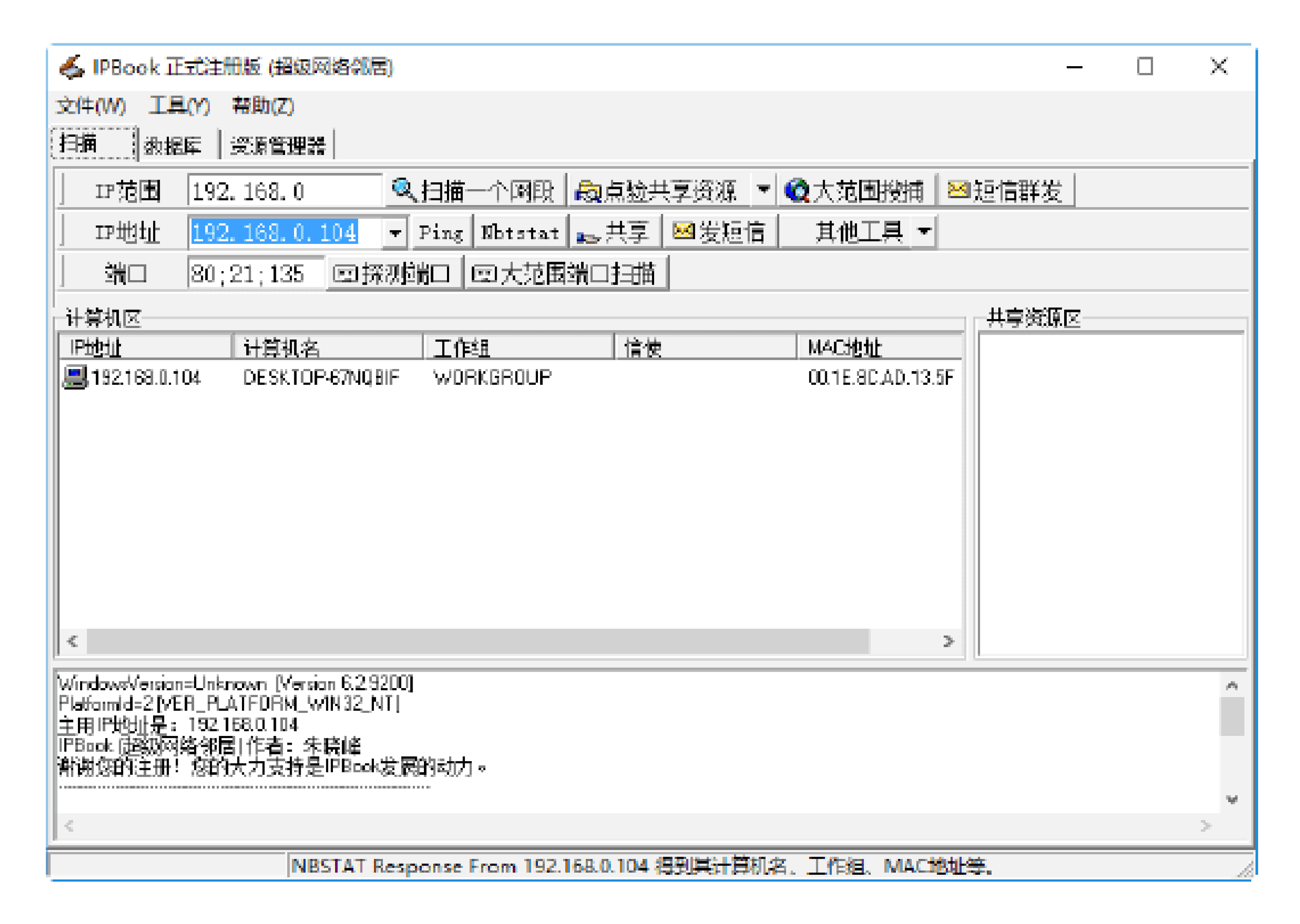
Step 05 单击“确定”按钮，即可打开该主机的网络共享文件夹，在其中查看共享信息，如下图所示。



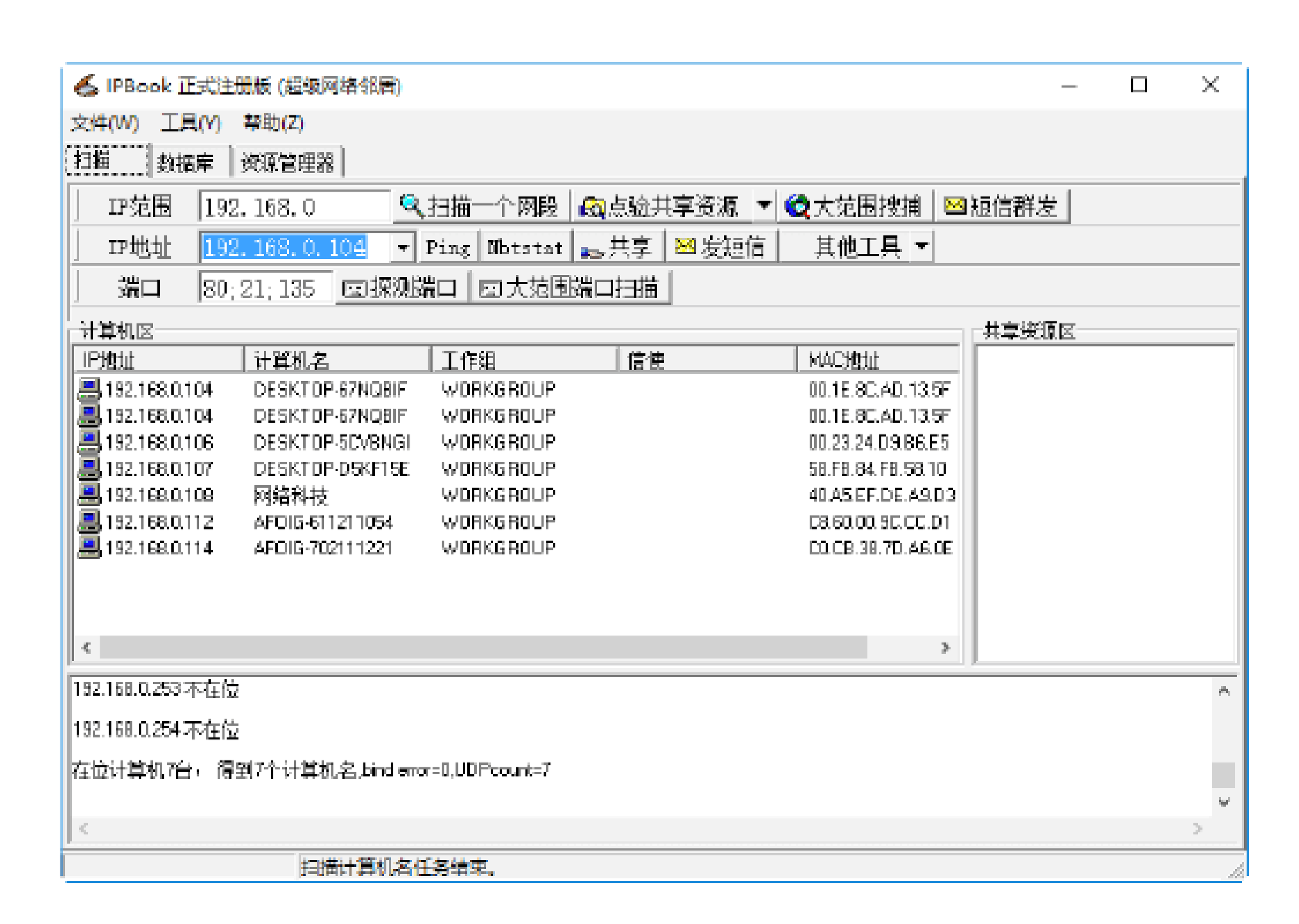
实战2：使用IPBook查看

IPBook（超级网络邻居）是一款小巧的搜索共享资源及FTP共享的工具，软件自解压后就能直接运行。它还有许多辅助功能，如发送短信等，并且所有功能不限于局域网，可以在互联网使用。使用该工具的具体操作步骤如下。

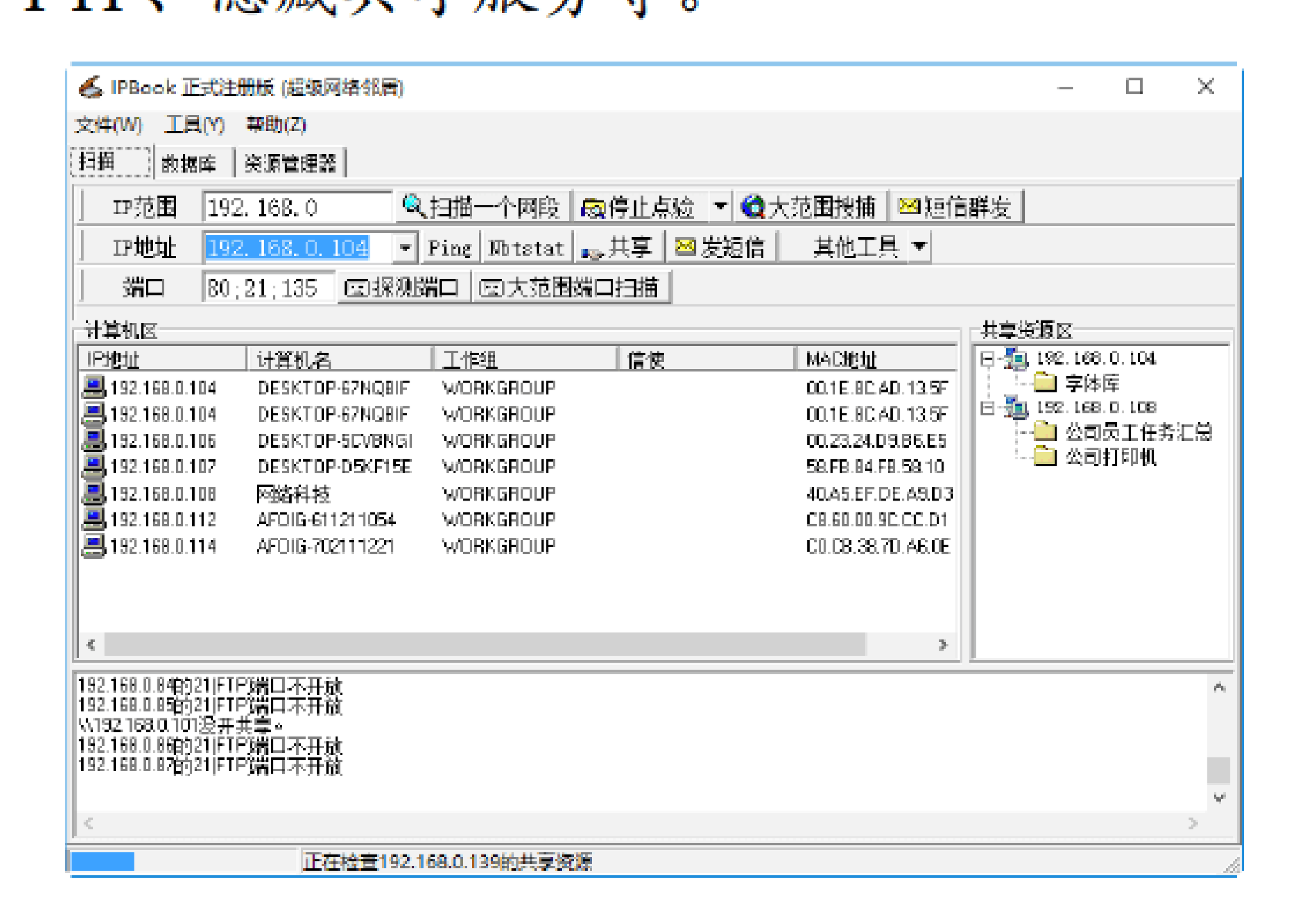
Step 01 双击下载的IPBook应用程序，打开“IPBook（超级网络邻居）”主窗口，在其中即可自动显示本机的IP地址和计算机名，如下图所示。其中192.168.0.104和192.168.0分别是本机的IP地址与本机所处局域网的IP范围。



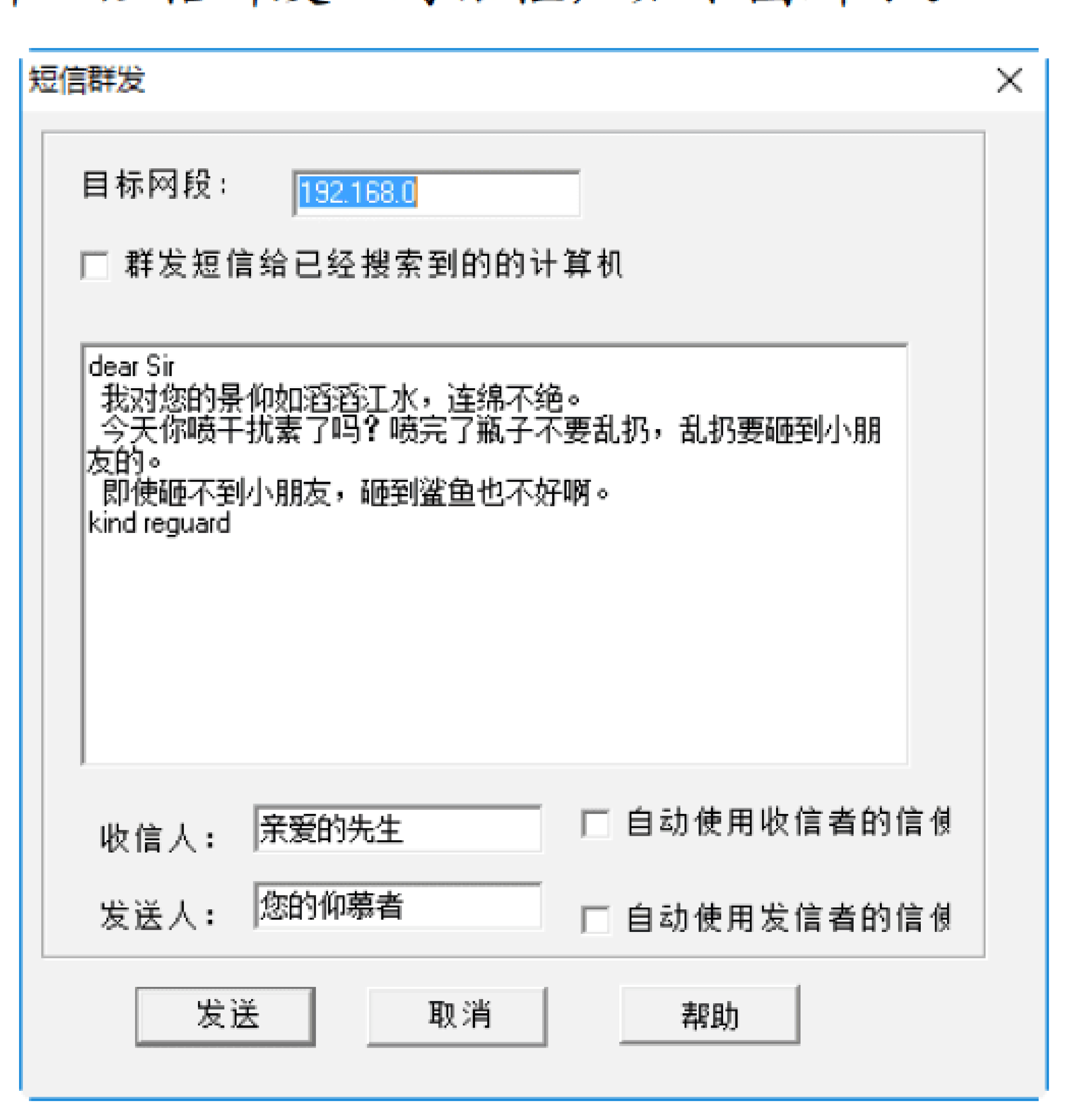
Step 02 在IPBook工具中可以查看本网段所有机器的计算机名与共享资源。在“IPBook（超级网络邻居）”主窗口中，单击“扫描一个网段”按钮，几秒钟之后，本机所在局域网的所有在线计算机的详细信息将显示在左侧列表框中，如下图所示，其中包含IP地址、计算机名、工作组、信使等信息。



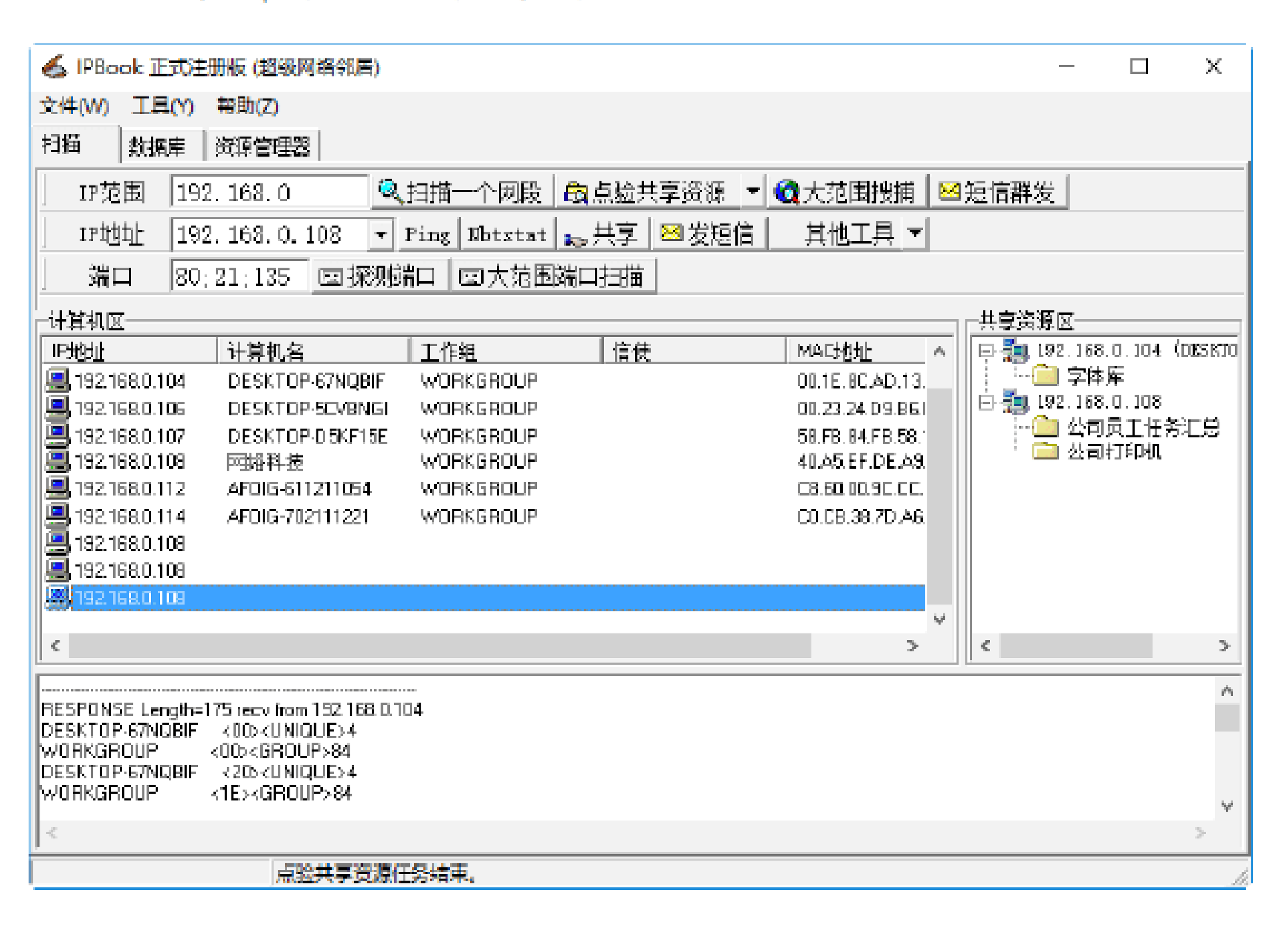
Step 03 在显示出所有计算机信息后，单击“点验共享资源”按钮，即可查出本网段机器的共享资源，并将搜索的结果显示在右侧的树状显示框中，如下图所示，在搜索之前还可以设置是否同时搜索HTTP、FTP、隐藏共享服务等。



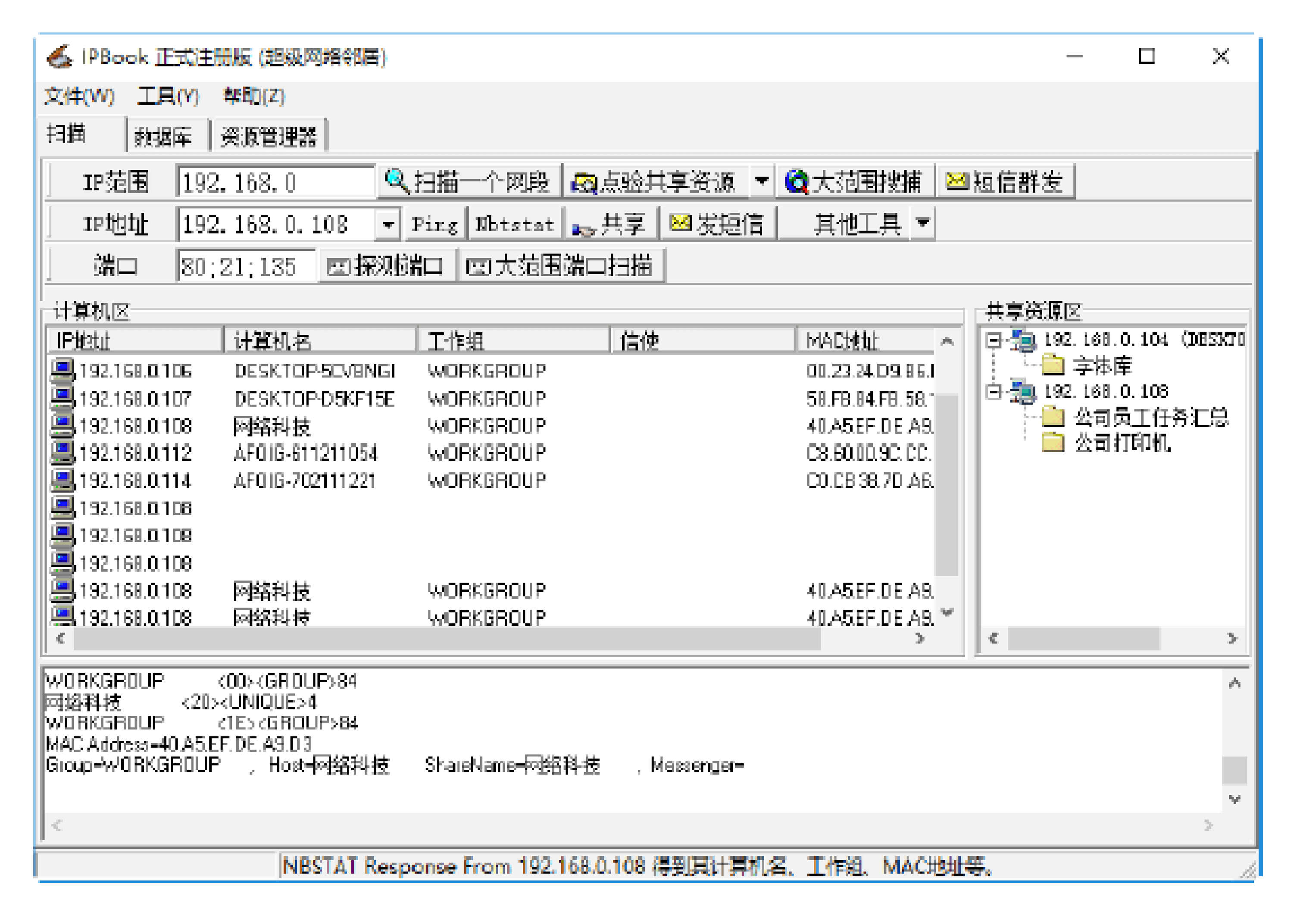
Step 04 在IPBook工具中还可以给目标网段发送短信，在“IPBook（超级网络邻居）”主窗口中单击“短信群发”按钮，即可打开“短信群发”对话框，如下图所示。



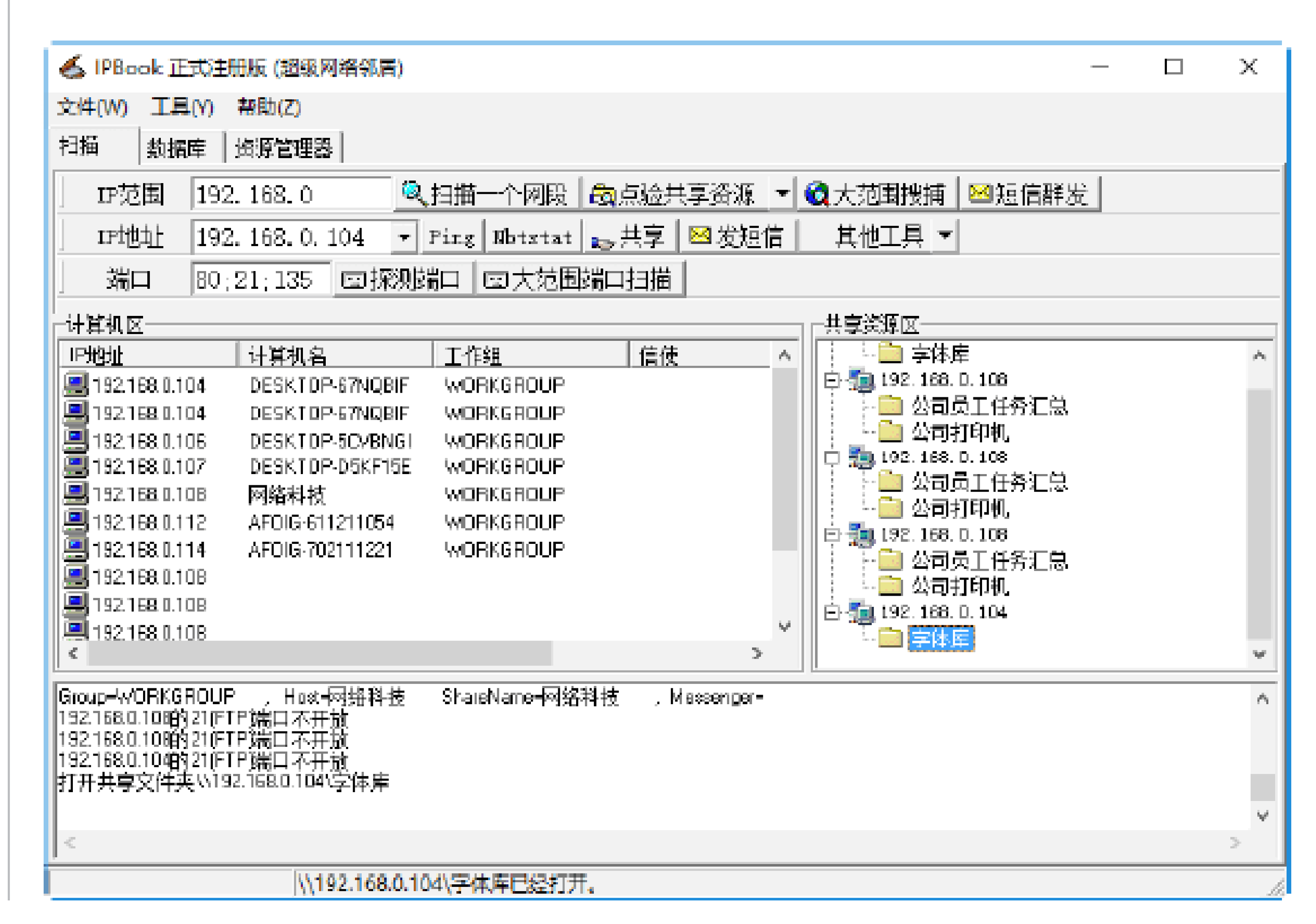
Step 05 在“计算机区”列表中选择某台计算机，单击Ping按钮，即可在“IPBook（超级网络邻居）”主窗口看到该命令的运行结果，如下图所示。根据得到的信息来判断目标计算机的操作系统类型。



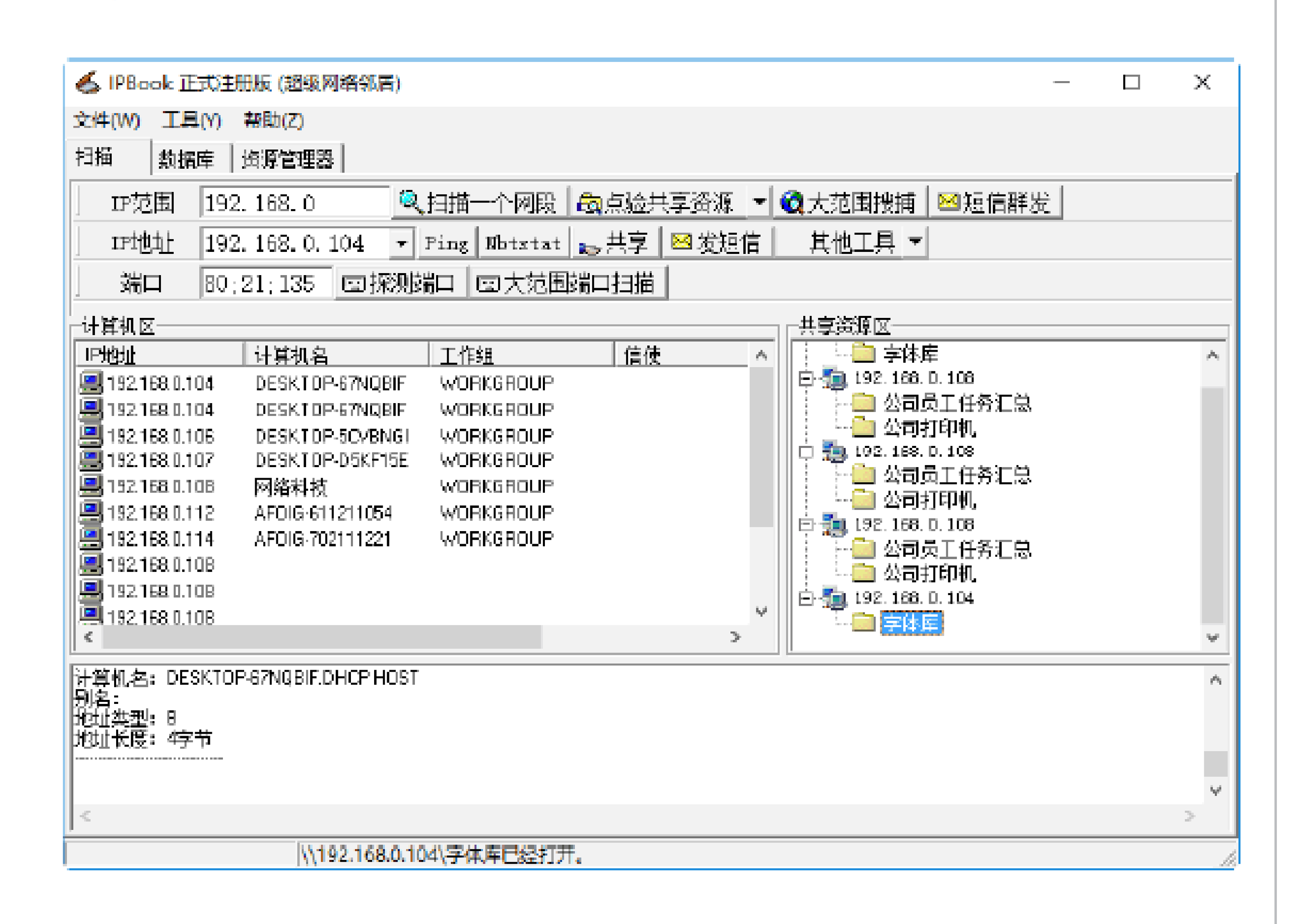
Step 06 在“计算机区”列表中选择某台计算机，单击Nbtstat按钮，即可在“IPBook（超级网络邻居）”主窗口看到该主机的计算机名称，如下图所示。



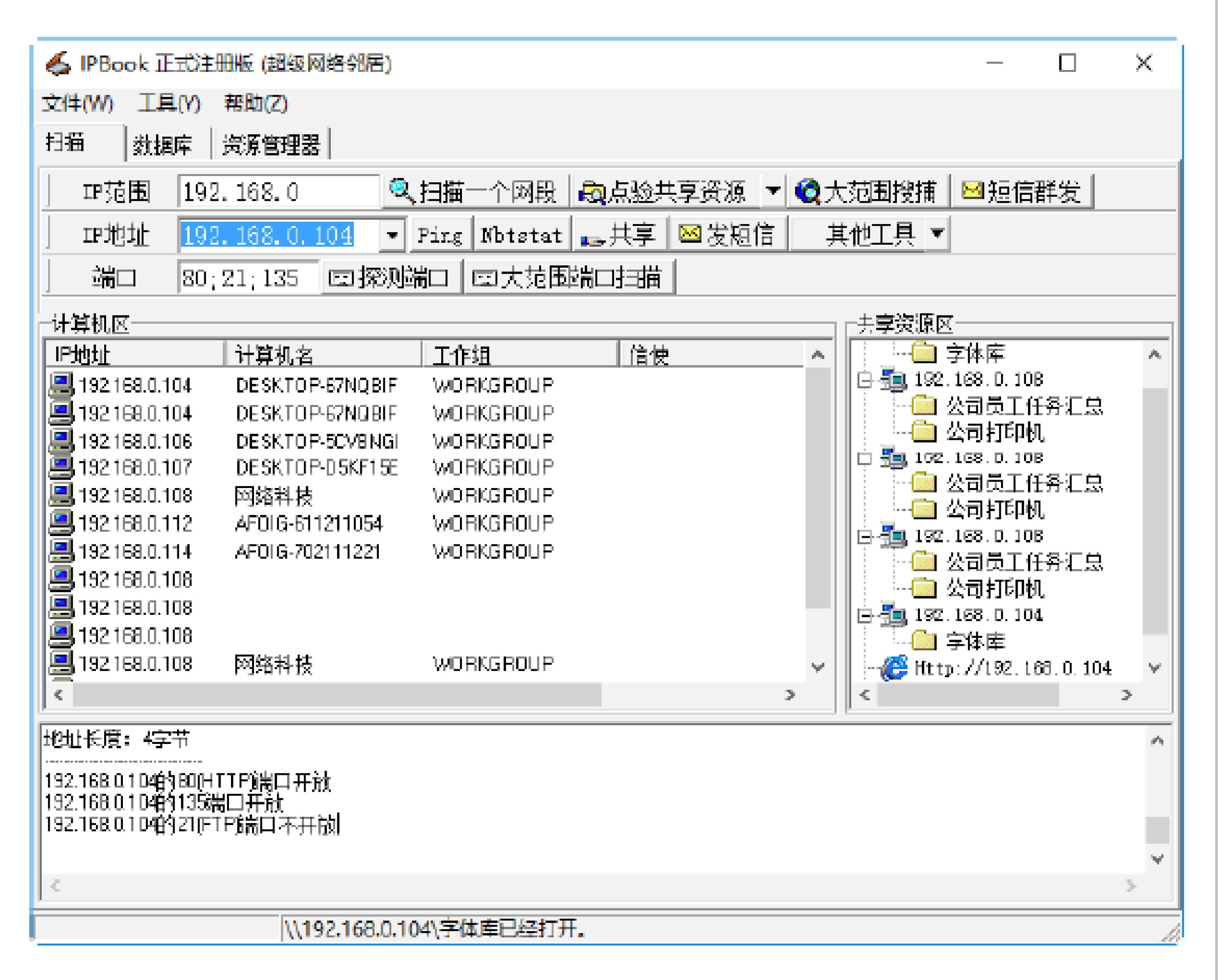
Step 07 单击“共享”按钮，即可对指定的网络段的主机进行扫描，并把扫描到的共享资源显示出来，如下图所示。



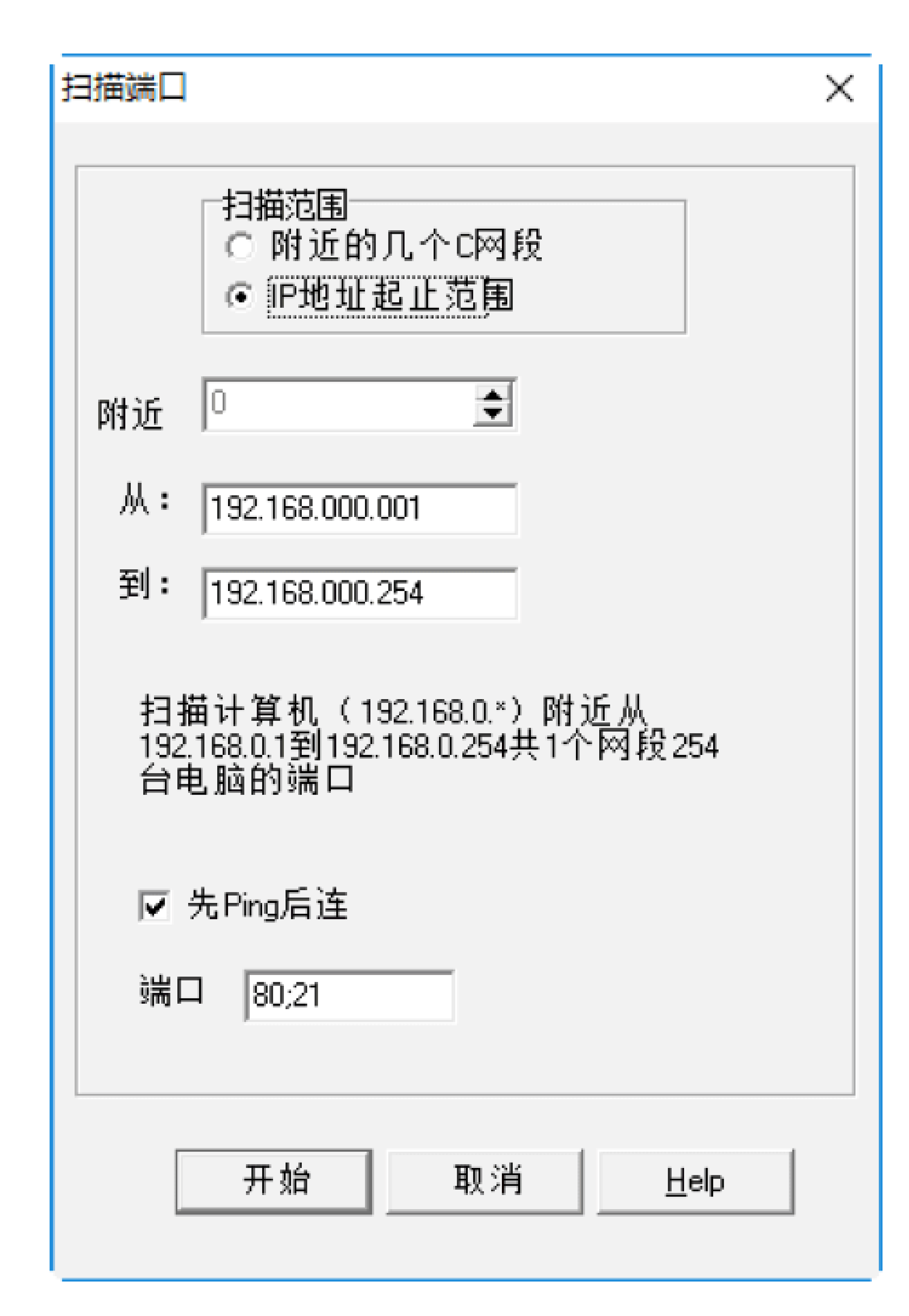
Step 08 IPBook工具还具有将域名转换为IP地址的功能，在“IPBook（超级网络邻居）”主窗口中单击“其他工具”按钮，在弹出的快捷菜单中选择“域名、IP地址转换”→“IP->Name”选项，即可将IP地址转换为域名，如下图所示。



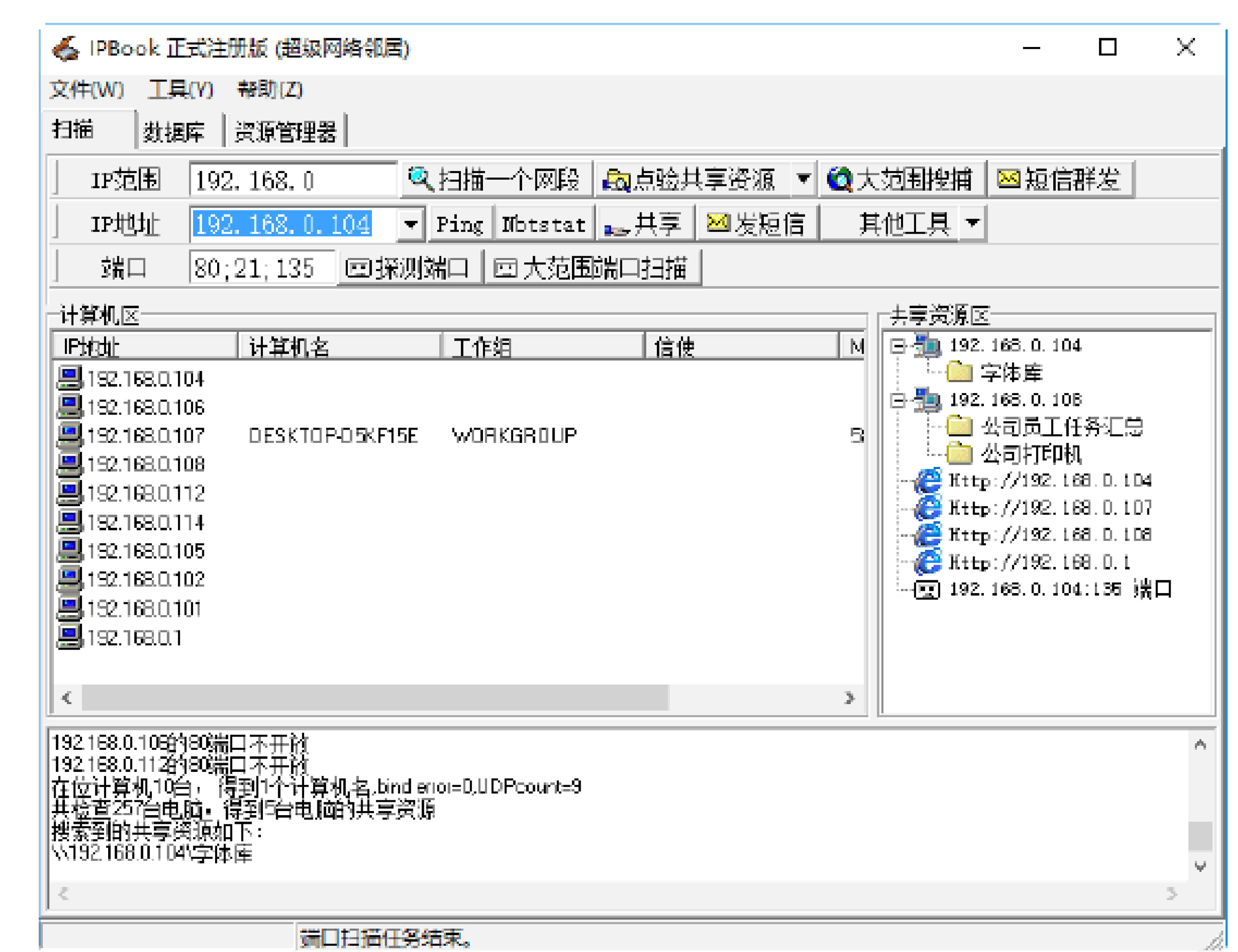
Step 09 单击“探测端口”按钮，即可探测整个局域网中各个主机的端口，同时将探测的结果显示在下面的列表中，如下图所示。



Step 10 单击“大范围端口扫描”按钮，即可打开“扫描端口”对话框，如下图所示。选中“IP地址起止范围”单选按钮，将要扫描的IP地址范围设置为192.168.000.001~192.168.000.254，最后将要扫描的端口设置为80；21。



Step 11 单击“开始”按钮，即可对设定IP地址范围内的主机进行扫描，同时将扫描到的主机显示在下面的列表中，如下图所示。



Step 12 在使用IPBook工具过程中，还可以对该软件的属性进行设置。在“IPBook（超级网络邻居）”主窗口中选择“工具”→“选项”选项，即可打开“设置”对话框，如下图所示。在“扫描设置”选项卡下，在其中即可设置“Ping设置”和“解析计算机名的方式”属性。



Step 13 选择“共享设置”选项卡，在其中即可设置最大扫描线程数、搜索共享时的顺带搜索项目等属性，如下图所示。



如果成功注册，就可以使用“大范围搜索”功能来搜索任意范围的计算机名、工作组、MAC地址及共享资源等。

9.3 局域网的安全防护

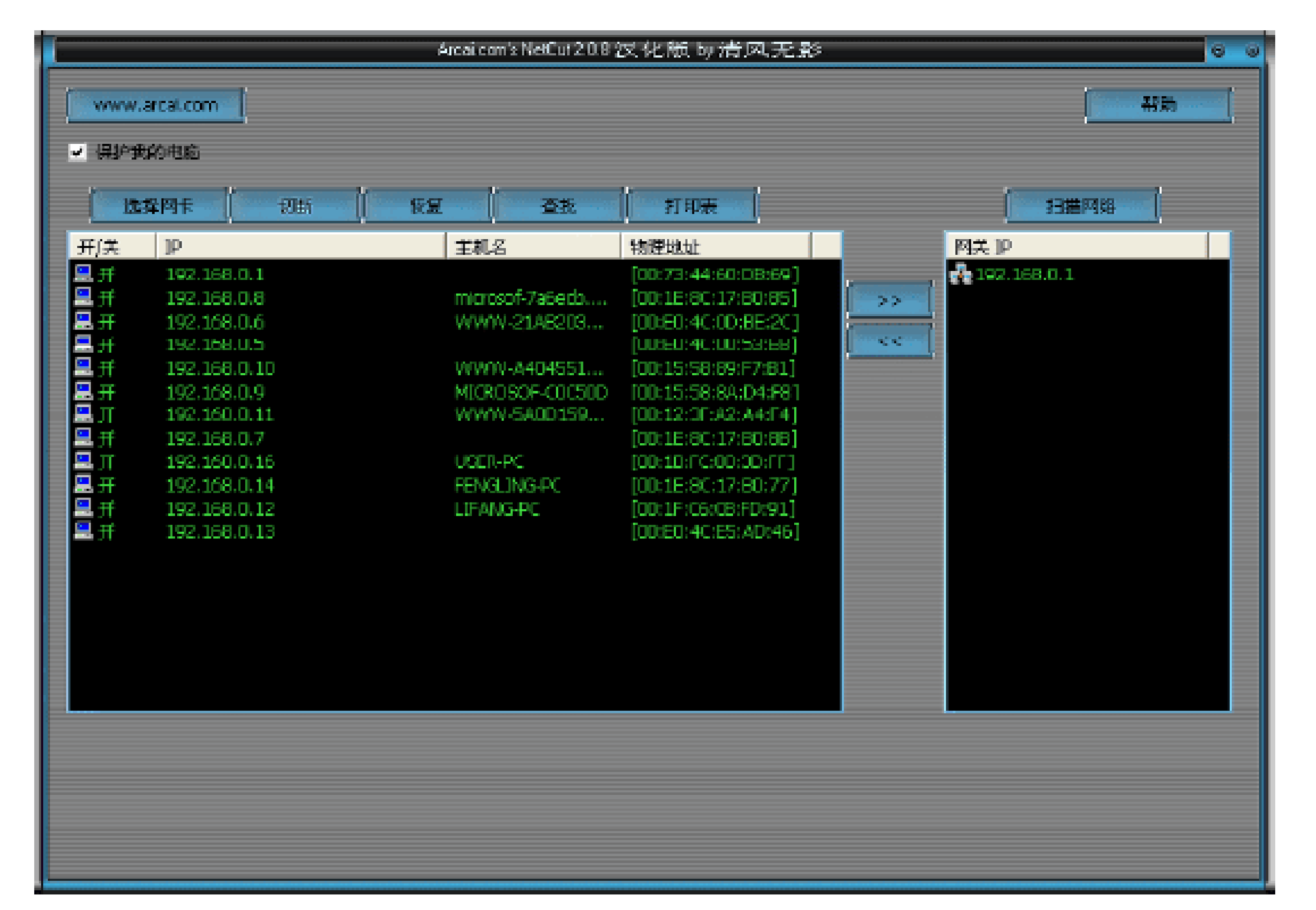
使用局域网攻击工具可以对局域网进行攻击，如利用ARP攻击工具可以使局域网中两台计算机的IP地址发生冲突，从而导致其中的一台计算机无法上网。常见的局域网攻击工具有网络剪刀手、网络特工等。

实战3：使用“网络剪刀手”切断网络

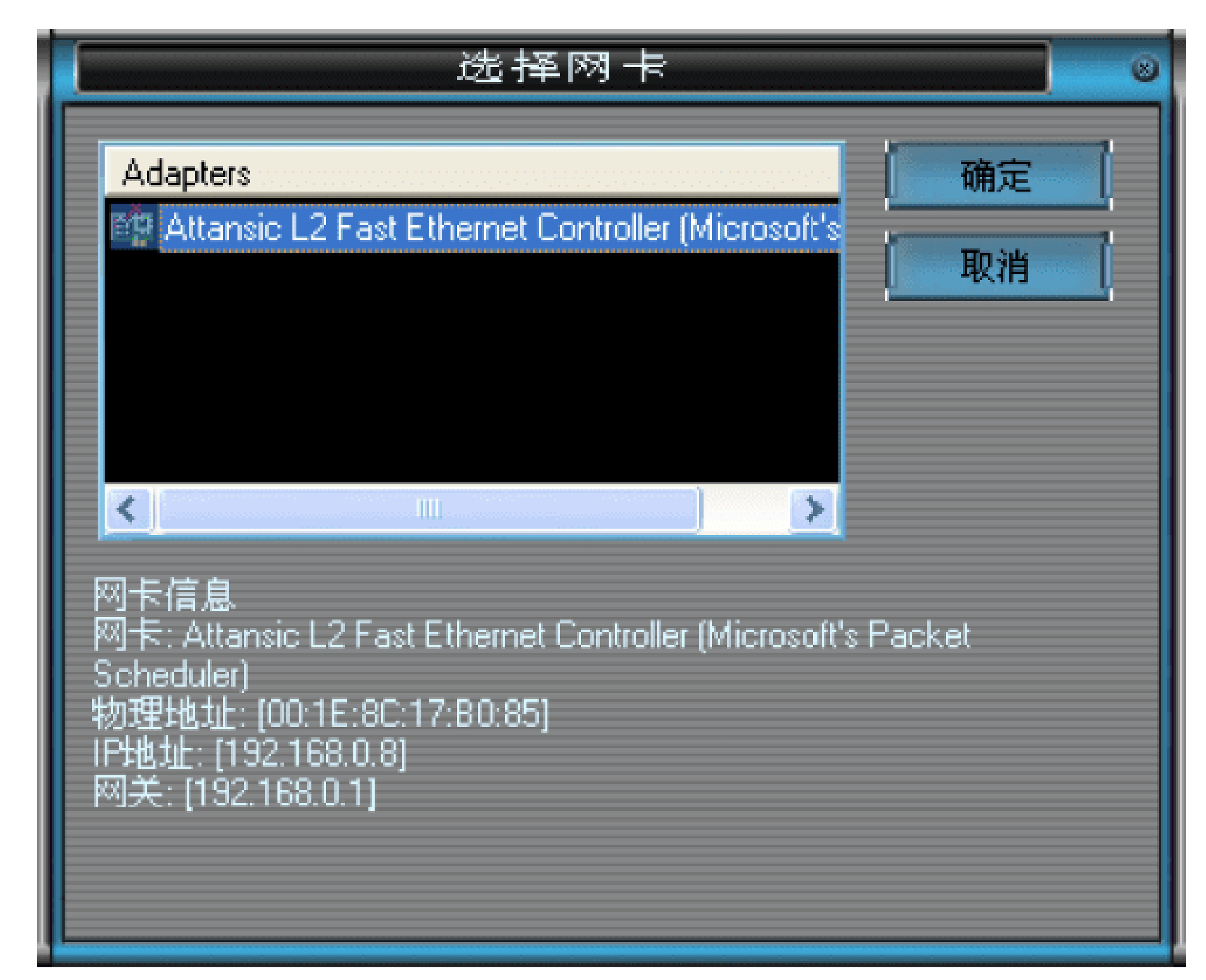
“网络剪切手Netcut”是一款网管必备工具，可以切断局域网里任何主机，使其断开网络连接。利用ARP协议，可以看到局域网内所有主机的IP地址。

该工具的具体使用步骤如下。

Step 01 下载并安装“网络剪切手”，然后双击其快捷图标，即可打开Netcut主窗口，软件会自动搜索当前网段内的所有主机的IP地址、计算机名以及各自对应的MAC地址，如下图所示。

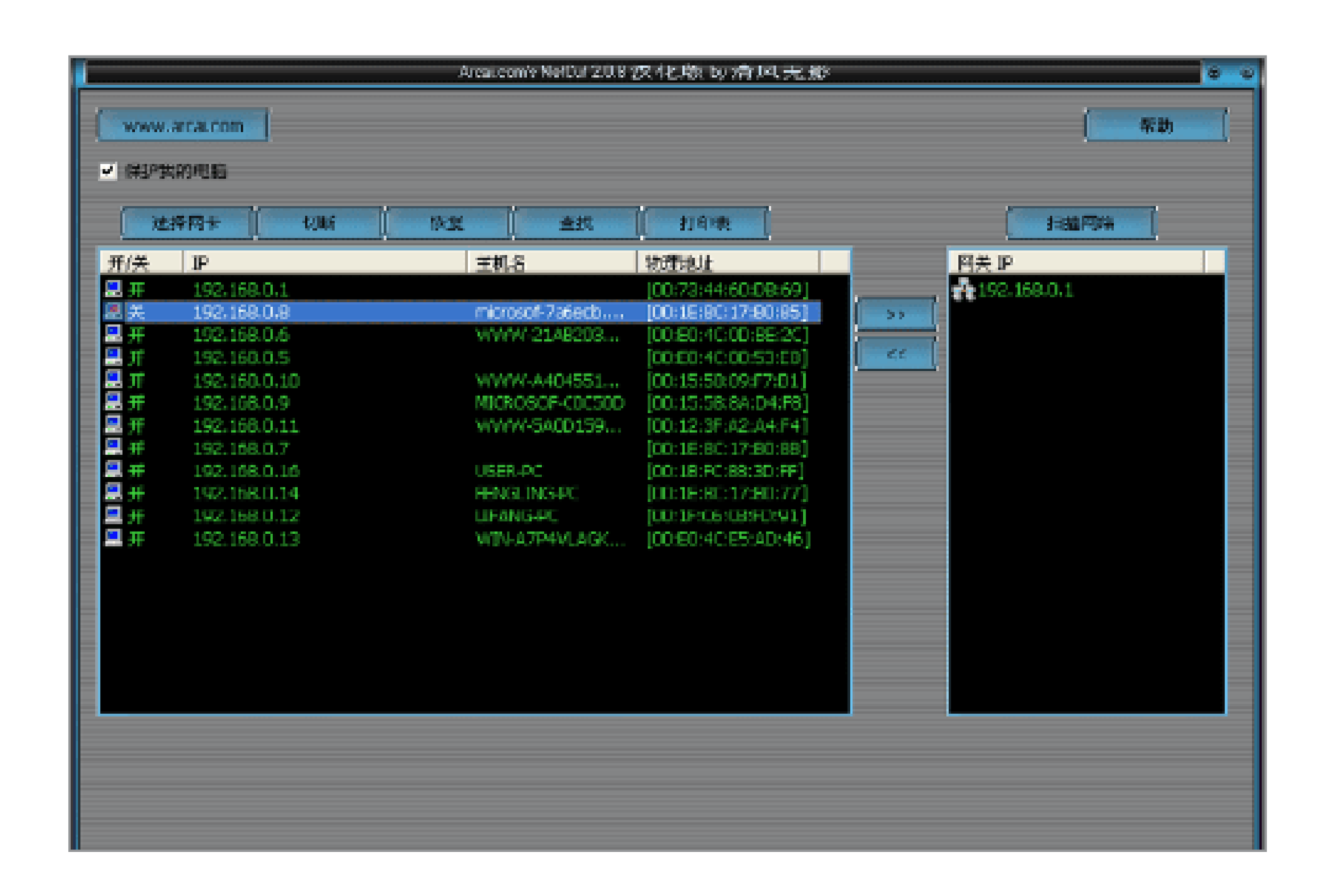


Step 02 单击“选择网卡”按钮，打开“选择网卡”对话框，在其中可以选择搜索计算机及发送数据包所使用的网卡，如下图所示。

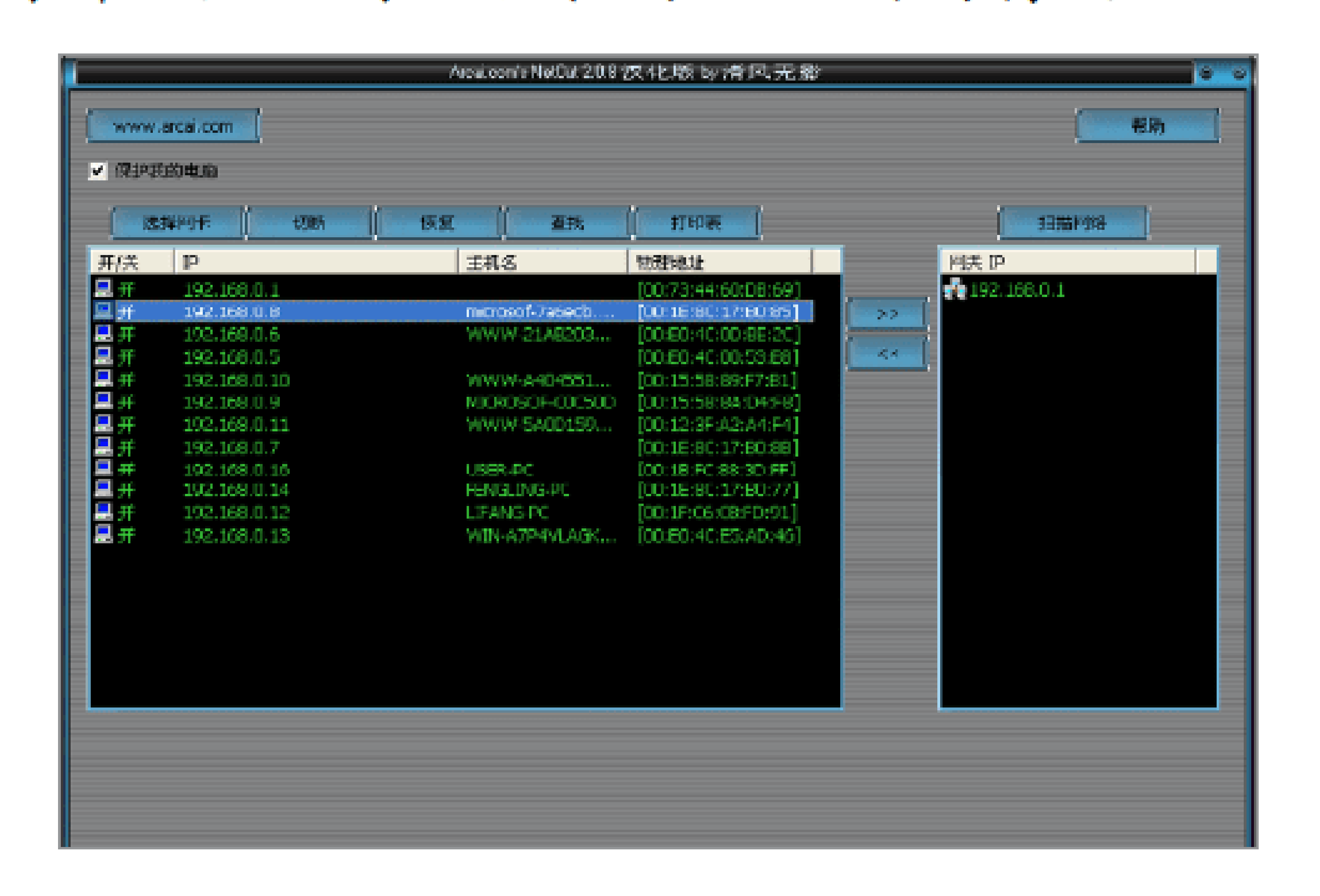


Step 03 在“网络剪刀手”中还可以开启或关闭局域网内任意主机对网关的访问。在扫描出的主机列表中，选中IP地址为192.168.0.8的主机，单击“切断”按钮，即可看到该主机的“开/关”状态已经变为“关”，如下图所示，此时该主机不能访问网关也不能打开网页。





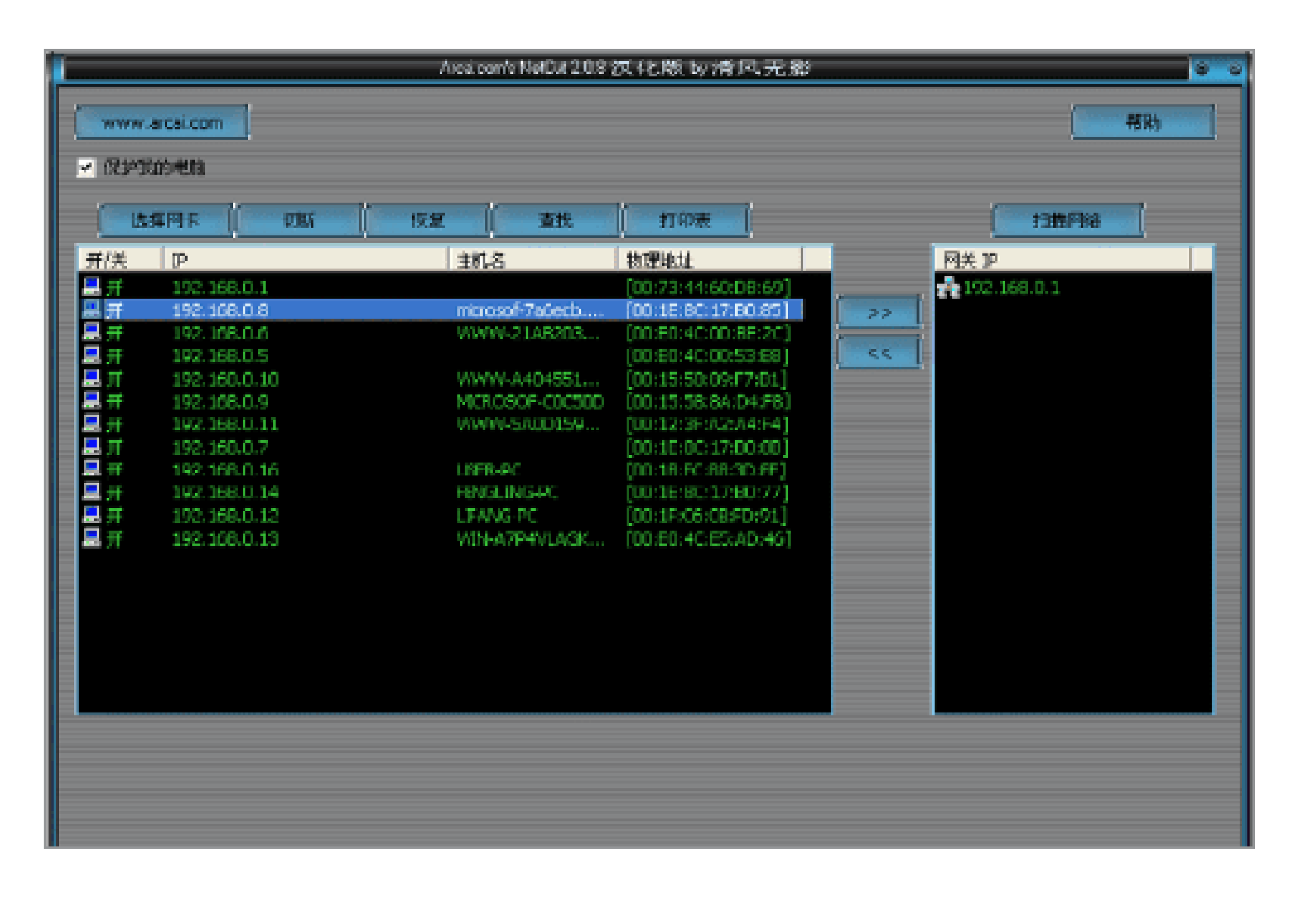
Step 04 再次选中IP地址为192.168.0.8的主机，单击“恢复”按钮，即可看到该主机的“开/关”状态又重新变为“开”，如下图所示，此时该主机可以访问因特网。



Step 05 如果局域网中主机过多的话，可以使用该工具提供的查找功能，快速查看某个主机的信息。在Netcut主窗口中单击“查找”按钮，即可打开“查找”对话框，如下图所示。

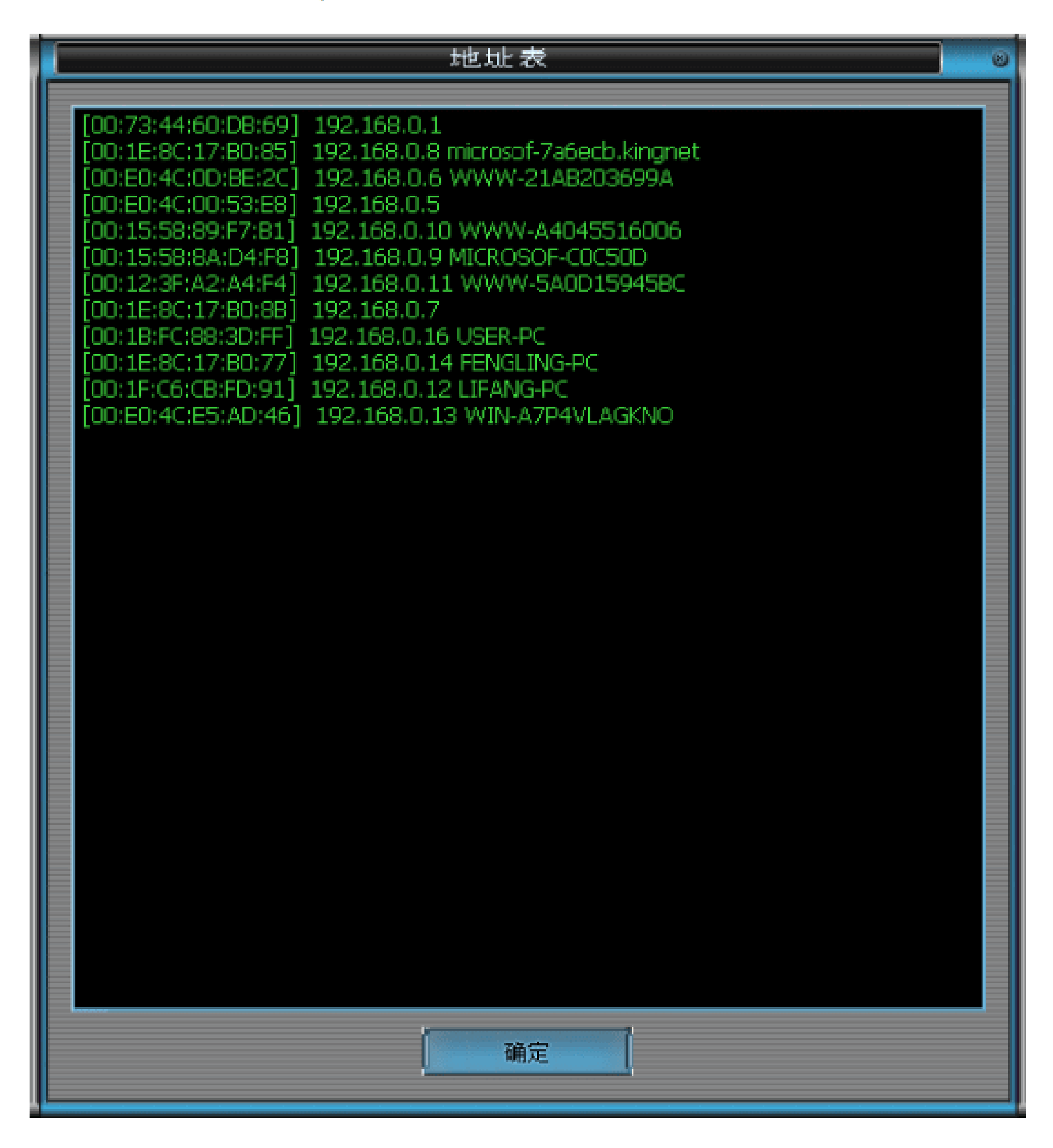


Step 06 在其中的文本框中输入要查找主机的某个信息，这里输入的是IP地址，然后单击“查找”按钮，即可在Netcut主窗口中快速找到IP地址为192.168.0.8的主机信息，如下图所示。

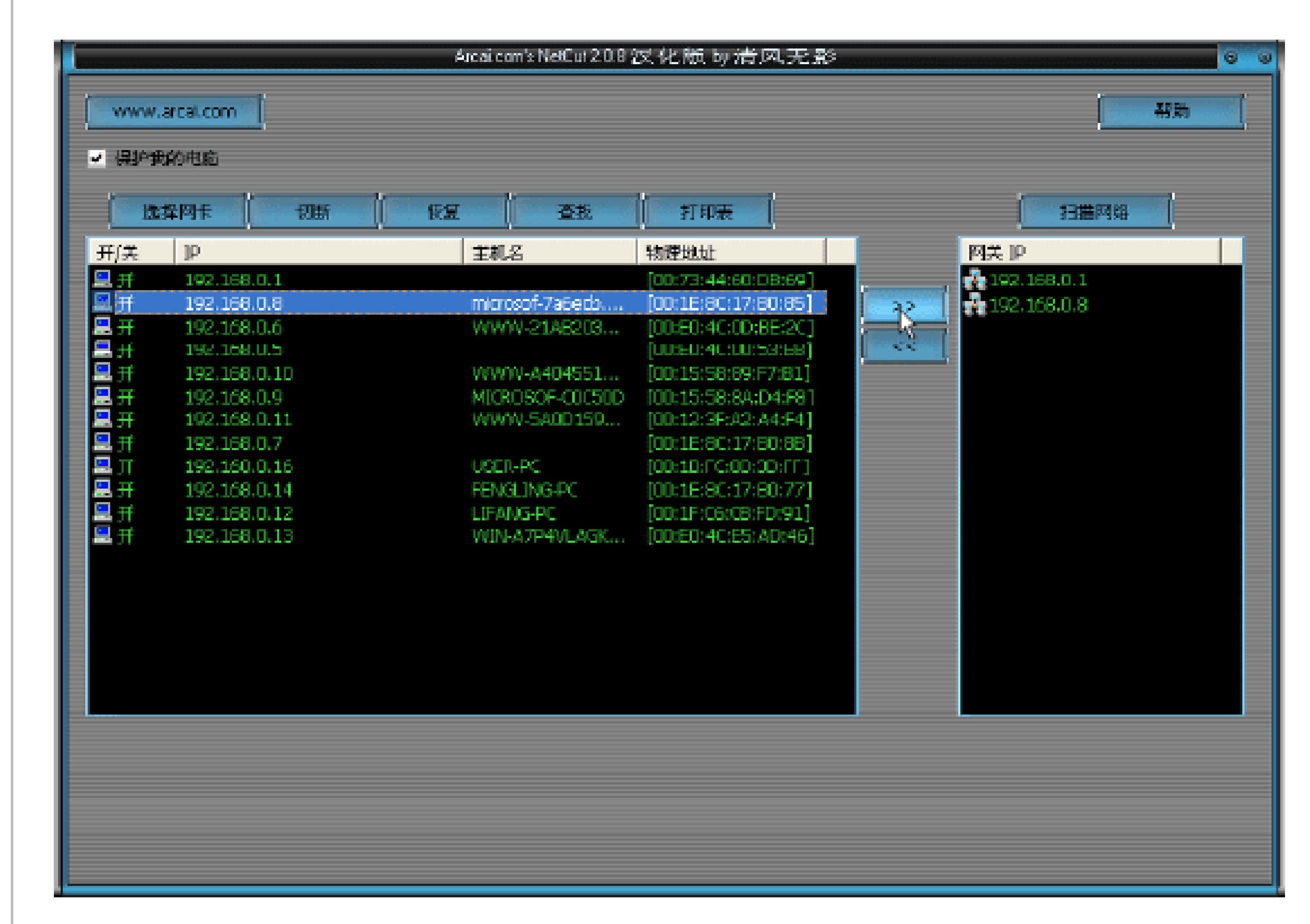




Step 07 利用“网络剪刀手”的“打印表”功能即可查看局域网中所有主机的信息。在Netcut主窗口中单击“打印表”按钮，即可打开“地址表”对话框，在其中即可看到所在局域网中所有主机的MAC地址、IP地址、用户名等信息，如下图所示。



Step 08 在“网络剪刀手”工具中还可以将某个主机的IP地址设置成网关IP地址。在Netcut主窗口中选择某台主机，单击 按钮“添加”按钮，将其IP地址添加到“网关IP”列表中，如下图所示。



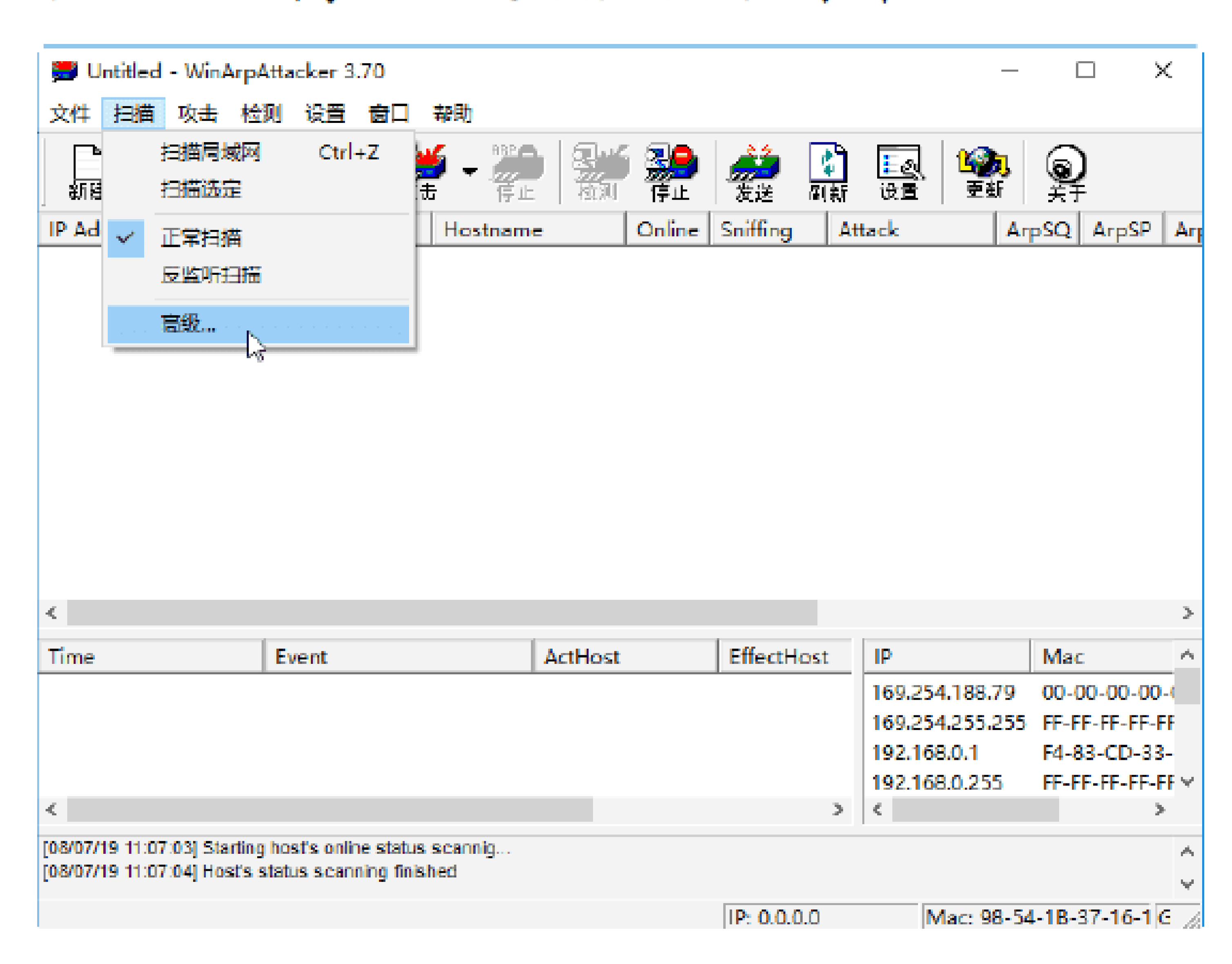
实战4：局域网中的ARP攻击

使用WinArpAttacker工具可以对局域网进行ARP攻击。WinArpAttacker是一款功能强大的局域网软件，利用该工具可以实现

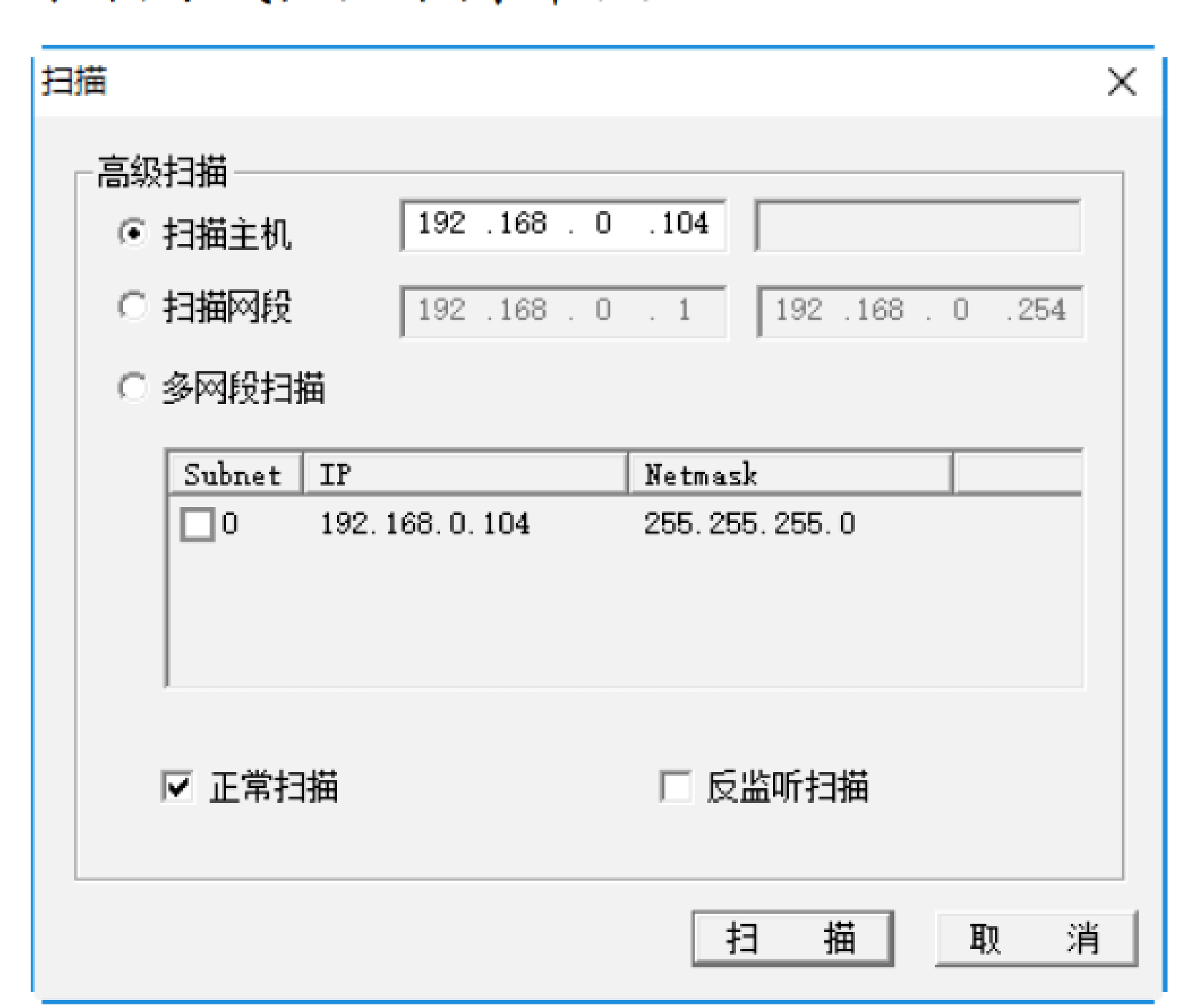
对ARP机器列表扫描，对ARP攻击、主机状态、本地ARP表发生变化等进行检测。

使用WinArpAttacker工具进行ARP攻击的具体操作步骤如下。

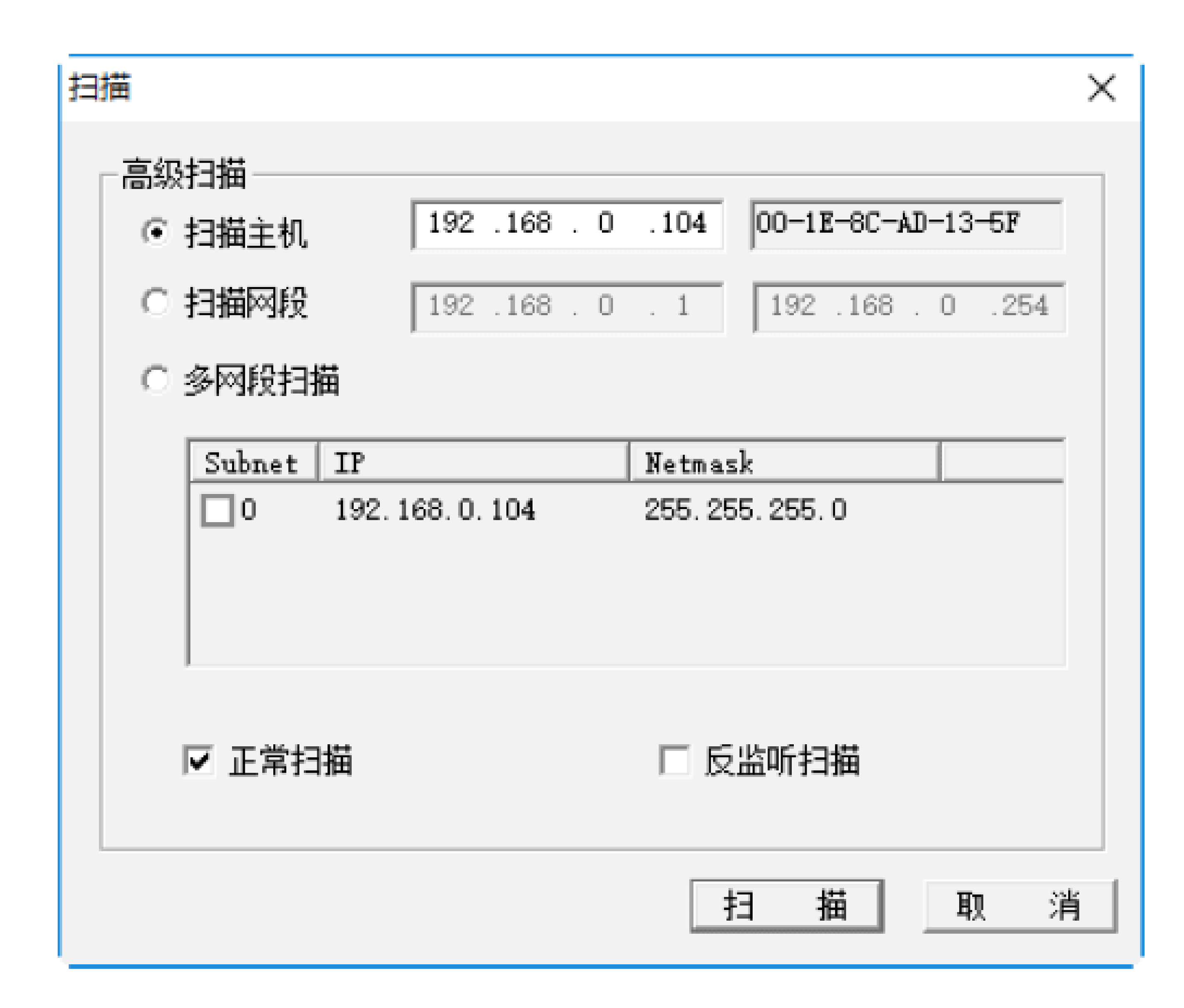
Step 01 下载WinArpAttacker软件，双击其中的WinArpAttacker.exe程序，即可打开WinArpAttacker主窗口，选择“扫描”→“高级”选项，如下图所示。



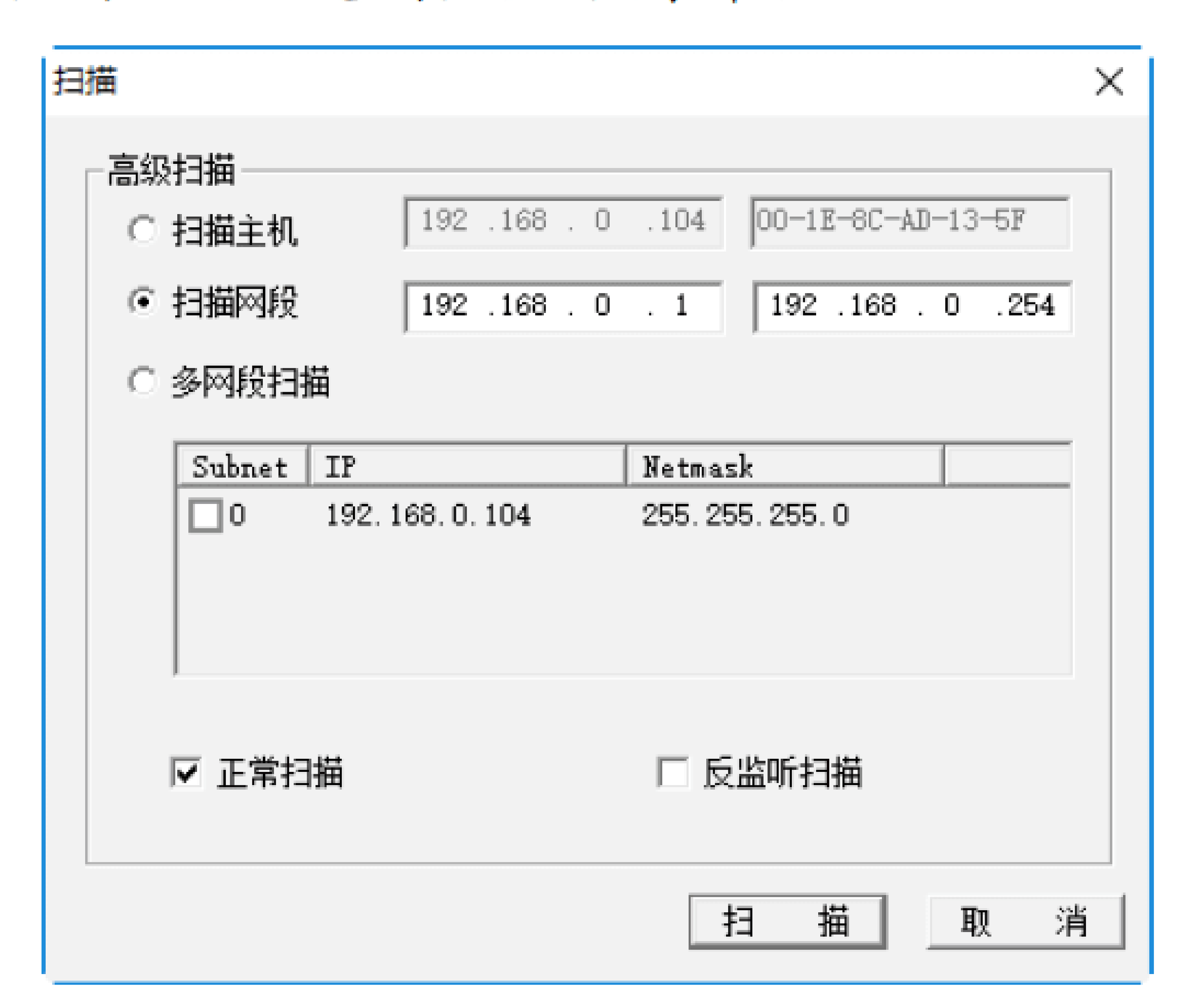
Step 02 打开“扫描”对话框，从中可以看出有扫描主机、扫描网段、多网段扫描等3种扫描方式，如下图所示。



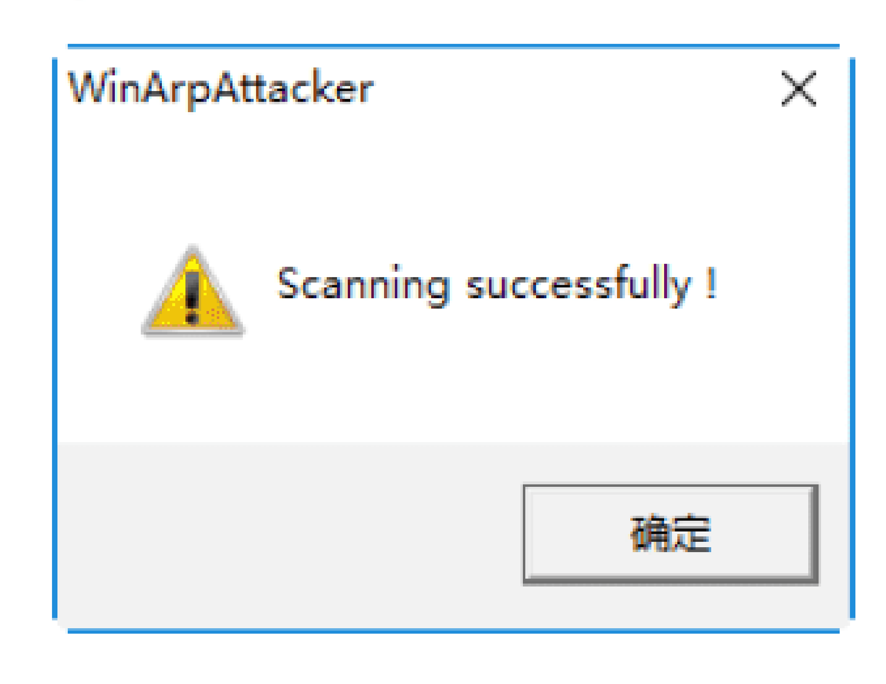
Step 03 使用“扫描主机”方式可以获得目标主机的MAC地址。在“扫描”对话框中选中“扫描主机”单选按钮，并在后面的文本框中输入目标主机的IP地址，如92.168.0.104，如下图所示，然后单击“扫描”按钮，即可获得该主机的MAC地址。



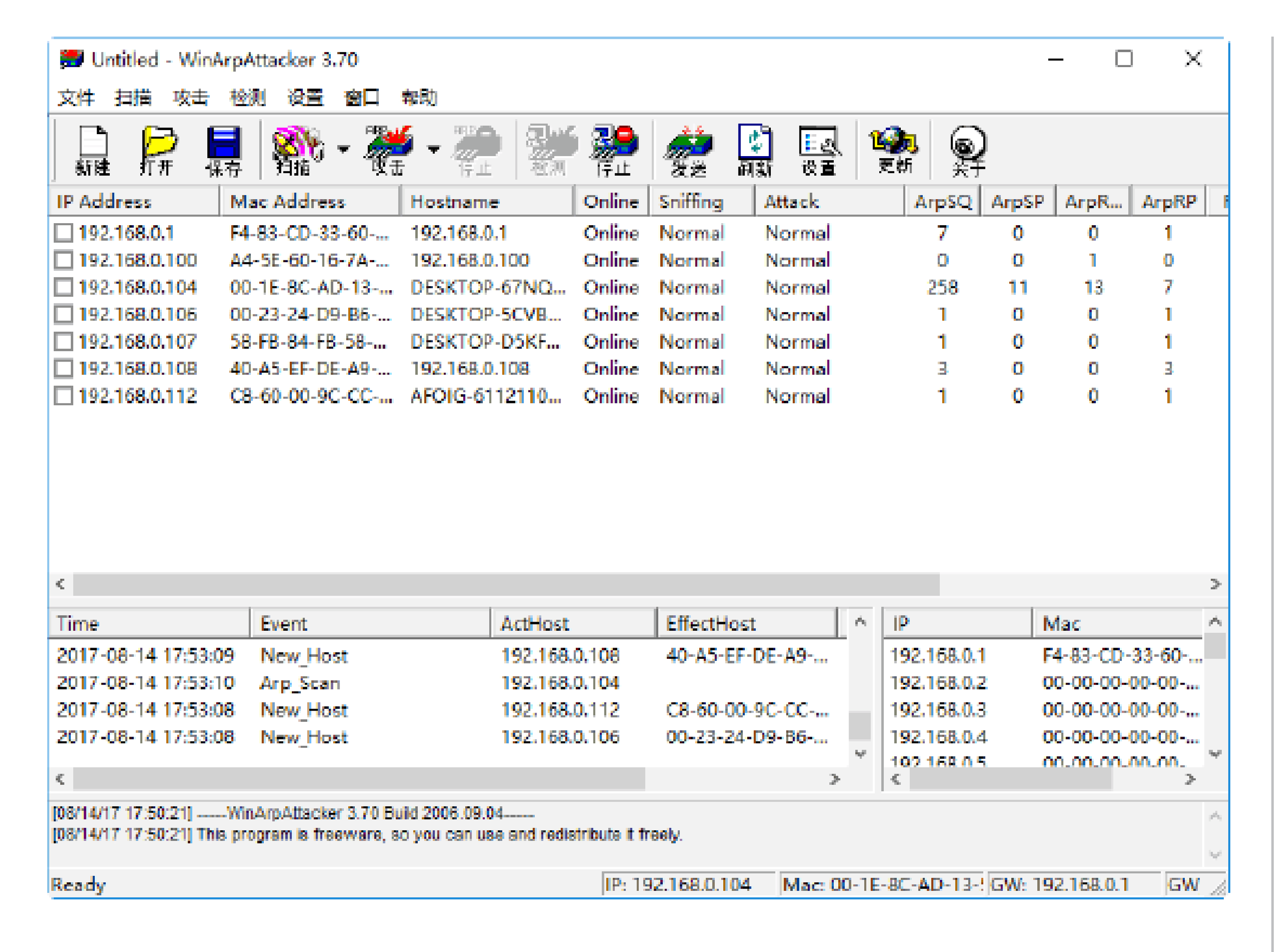
Step 04 “扫描网段”方式可以对指定IP段范围内的主机进行扫描。选中“扫描网段”单选按钮，在IP地址范围的文本框中输入扫描的IP地址范围，如下图所示。



Step 05 单击“扫描”按钮即可进行扫描操作，当扫描完成时会出现一个“Scaning successfully！”对话框，如下图所示。



Step 06 依次单击“确定”按钮，返回到WinArpAttacker主窗口中，在其中即可看到扫描结果，如下图所示。此时WinArpAttacker窗口被分成以下3个部分：

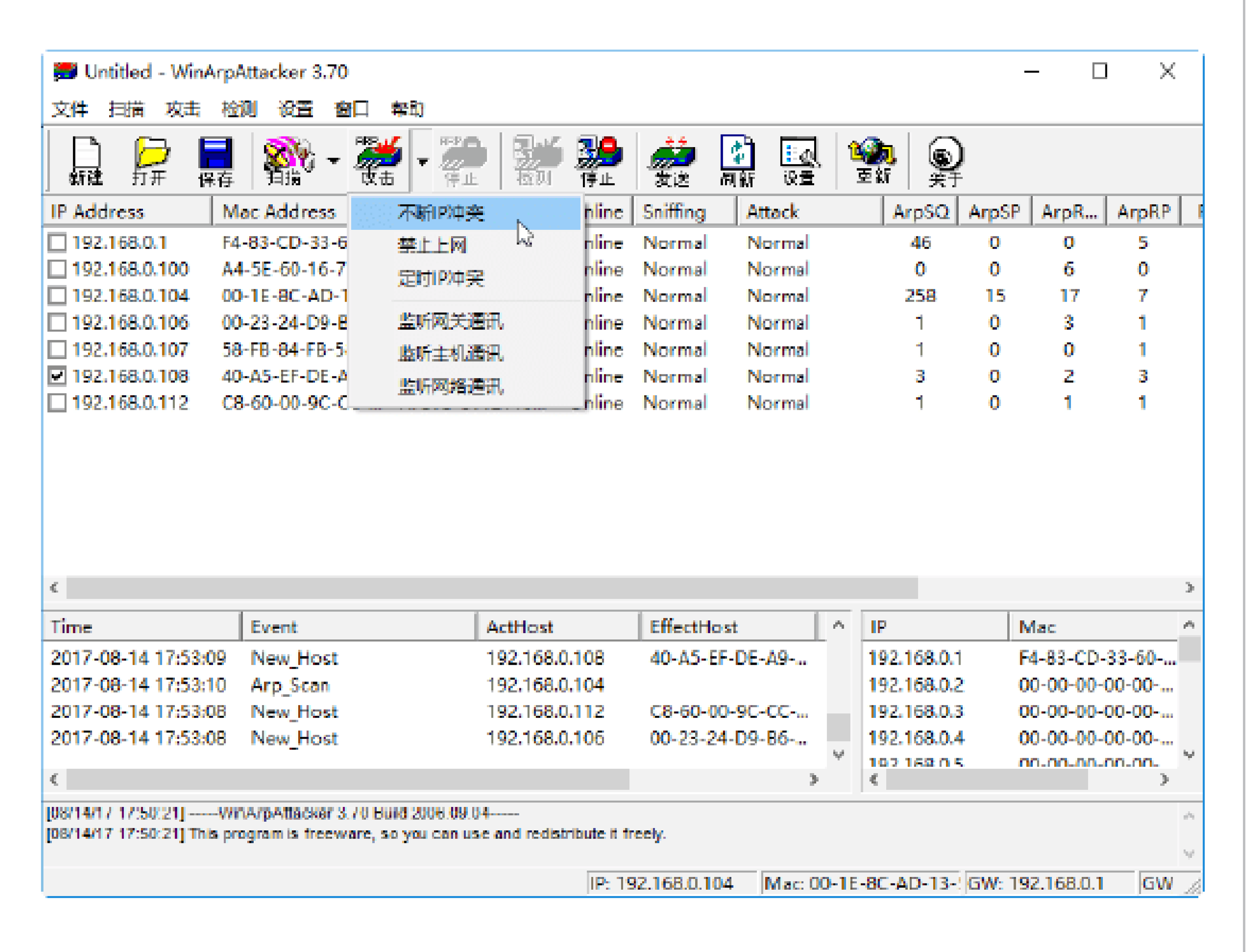


（1）上面的区域是主机列表区，主要显示局域网内的机器IP地址、MAC地址、主机名、是否在线、是否在监听、是否处于被攻击状态，以及ARP数据包和转发数据包统计信息等。

（2）左下方的区域是检测事件显示区，主要显示检测到的主机状态变化和攻击事件。

（3）右下方的区域显示IP地址和MAC地址信息。

Step 07 在扫描结果中勾选要攻击的目标计算机前面的复选框，然后在WinArpAttacker主窗口中单击“攻击”下拉按钮，在其弹出的快捷菜单中选择任意选项，就可以对其他计算机进行攻击了，如下图所示。



在WinArpAttacker中有以下6种攻击方式：

（1）不断IP冲突：不间断的IP冲突攻击，FLOOD攻击默认是一千次，可以在选项中改变这个数值。FLOOD攻击可使对方机器弹出IP冲突对话框，导致死机。

（2）禁止上网：禁止上网，可使对方机器不能上网。

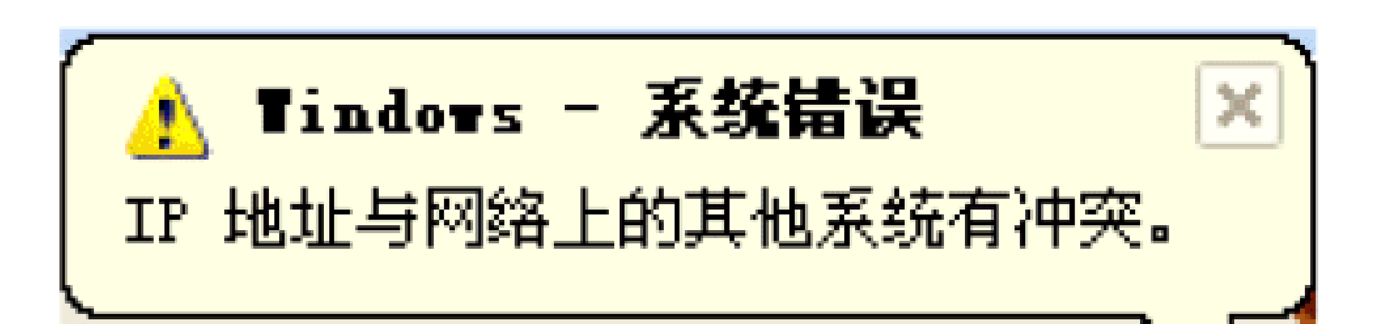
（3）定时IP冲突：IP地址定时冲突。

（4）监听网关通信：监听选定机器与网关的通信，监听对方机器的上网流量。发动攻击后，用抓包软件来抓包看内容。

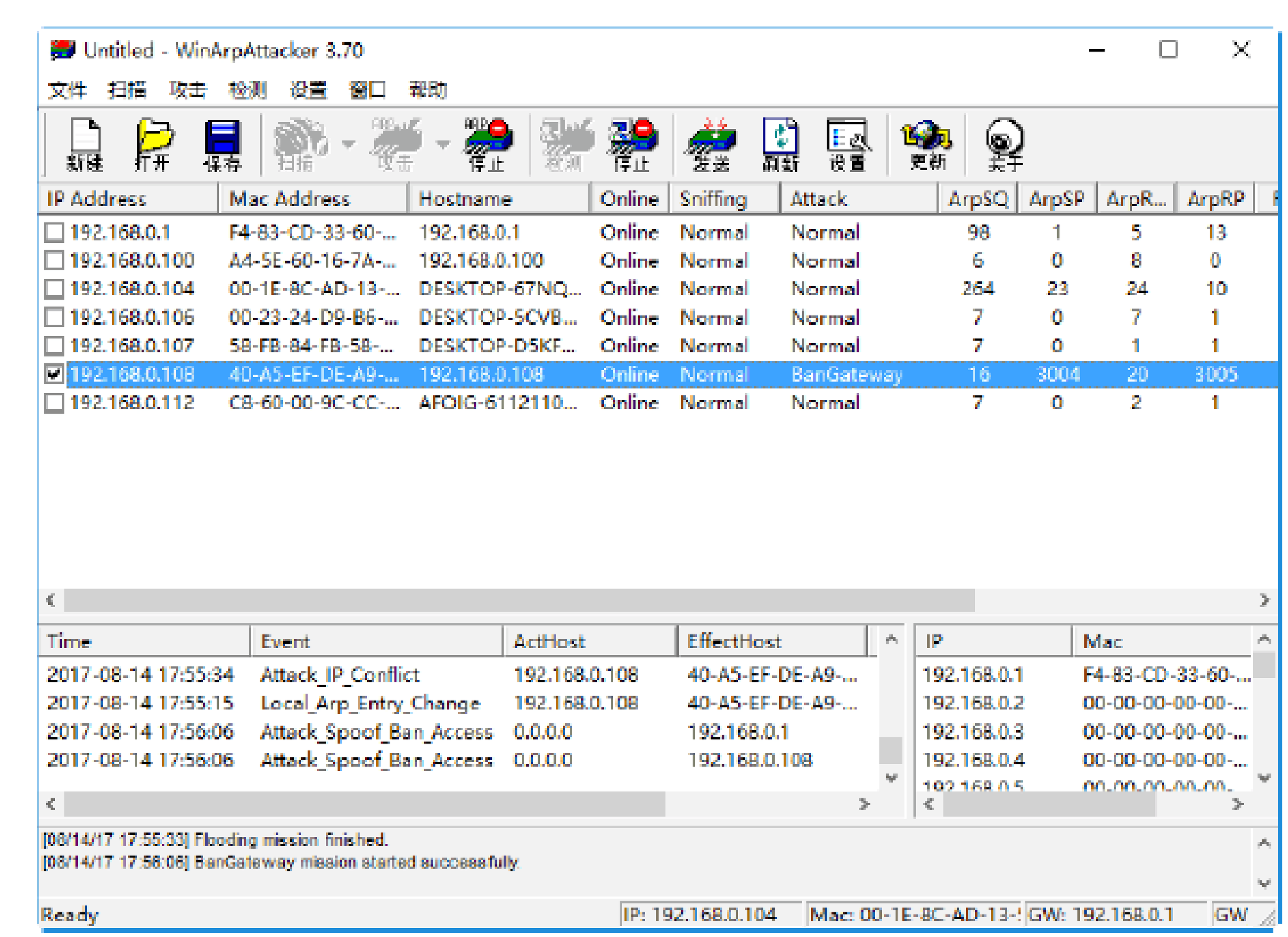
（5）监听主机通信：监听选定的几台机器之间的通信。

（6）监听网络通信：监听整个网络任意机器之间的通信，这个功能过于危险，可能会把整个网络搞乱，建议不要乱用。

Step 08 如果选择“IP冲突”选项，即可使目标计算机不断弹出“IP地址与网络上的其他系统有冲突”提示框，如下图所示。

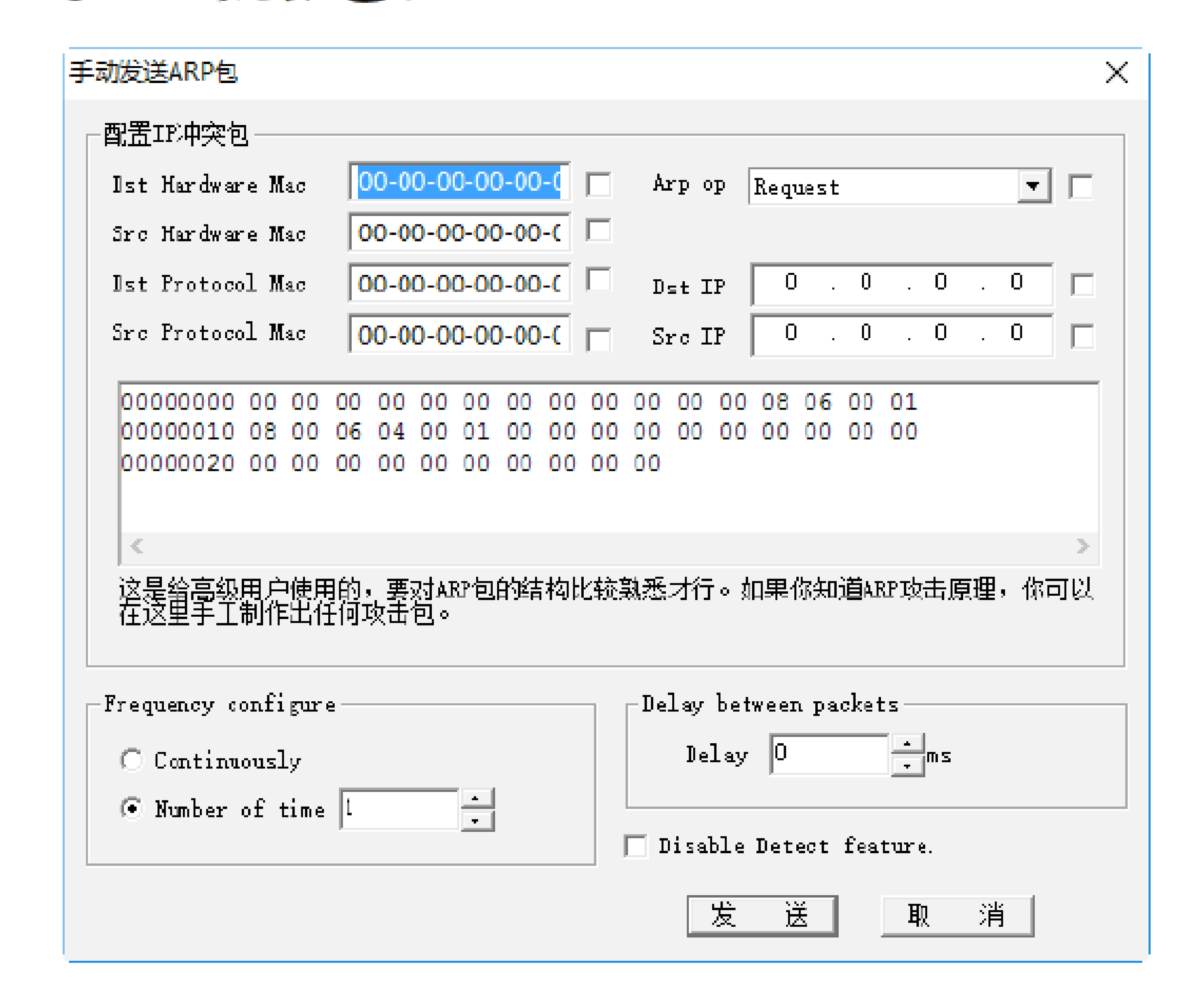


Step 09 如果选择“禁止上网”选项，此时在WinArpAttacker主窗口就可以看到该主机的“攻击”属性就变为BanGateway，如下图所示。如果想停止攻击，则需在WinArpAttacker主窗口选择“攻击”→“停止攻击”选项，否则将会一直进行。



Step 10 在WinArpAttacker主窗口单击“发送”按钮，即可打开“手动发送ARP包”对话框，在其中设置目标硬件Mac、Arp方向、源硬件Mac、目标协议Mac、源协议

Mac、目标IP和源IP等属性，如下图所示，单击“发送”按钮，即可向指定的主机发送ARP数据包。



Step 11 在WinArpAttacker主窗口中选择“设置”选项，然后在弹出的快捷菜单中选择任意一项，即可打开“Options”对话框，在其中对各个选项卡进行设置，如下图所示。

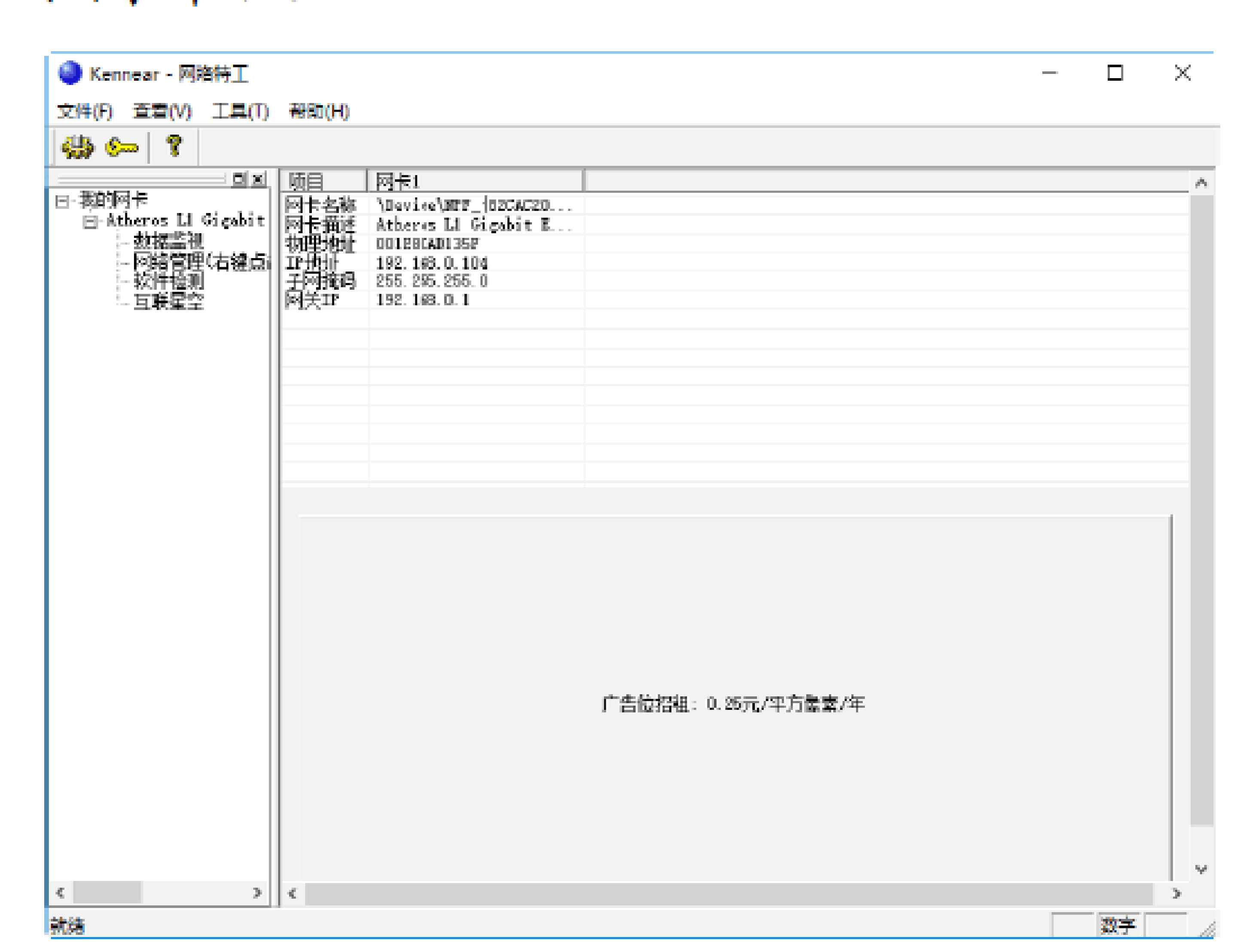
Options
适配器 攻击 更新 检测 分析 ARP代理 保护
网络配置
适配器 Atheros L1 Gigabit Ethernet 10/100/1
描述 Atheros L1 Gigabit Ethernet 10/100/100
本机 IP 192.168.0.104
子网掩码 255.255.255.0
本机 MAC 00-1E-8C-AD-13-5F
网关 IP 192.168.0.1
网关 MAC F4-83-CD-33-60-73
DNS 61.128.114.134
61.128.114.167
列表 \Device\NPF_{82CAC205-4844-4802-8E93-EC6F26B0D70F}
刷　新
确定 取消 应用(A)

实战5：监听局域网中的数据包

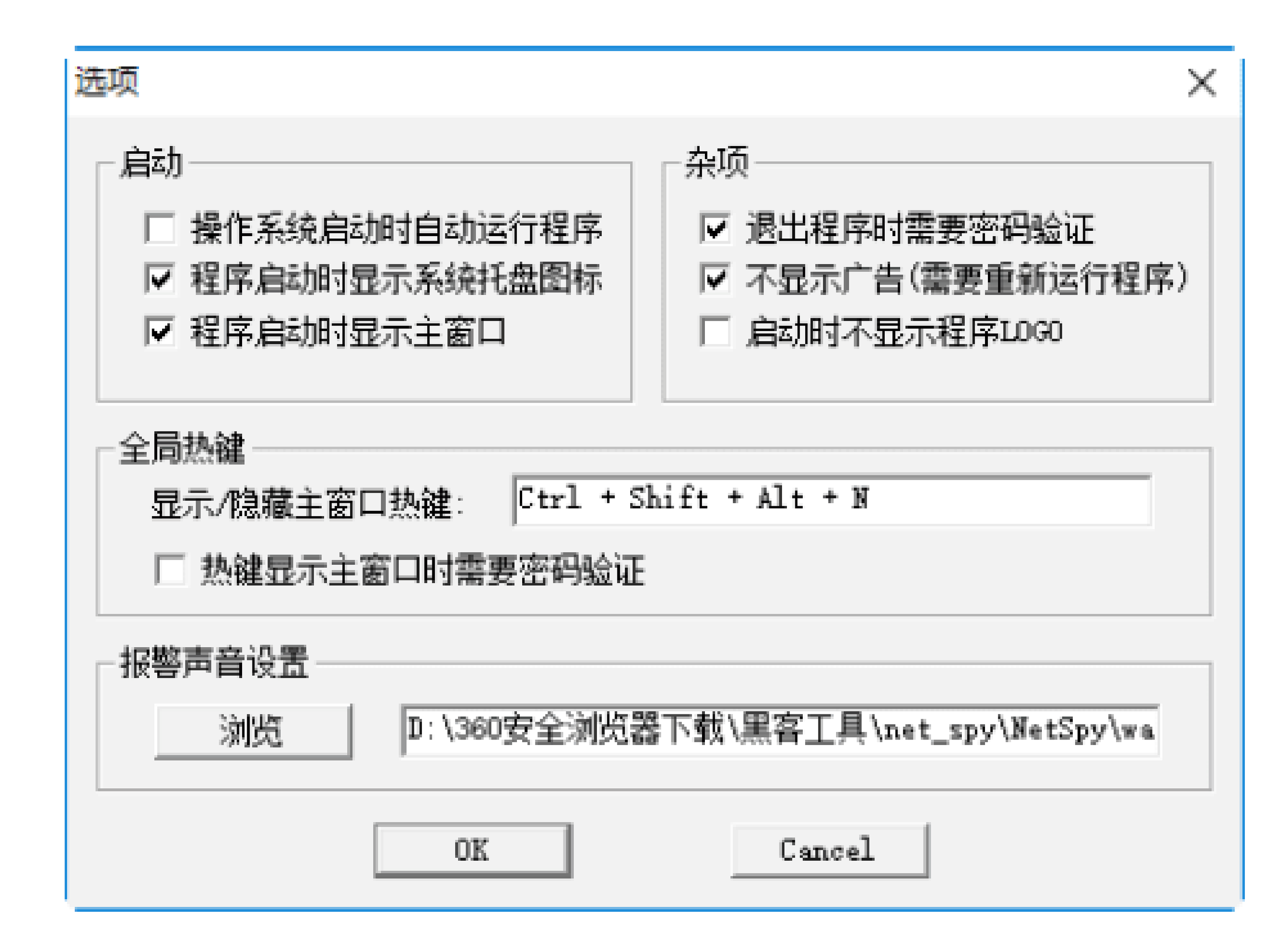
使用“网络特工”可以监听局域网中的数据包，如可以监视与主机相连HUB上所有机器收发的数据包；还可以监视所有局域网内的机器上网情况，以对非法用户进行管理，并使其登录指定的IP网址。

使用网络特工的具体操作步骤如下。

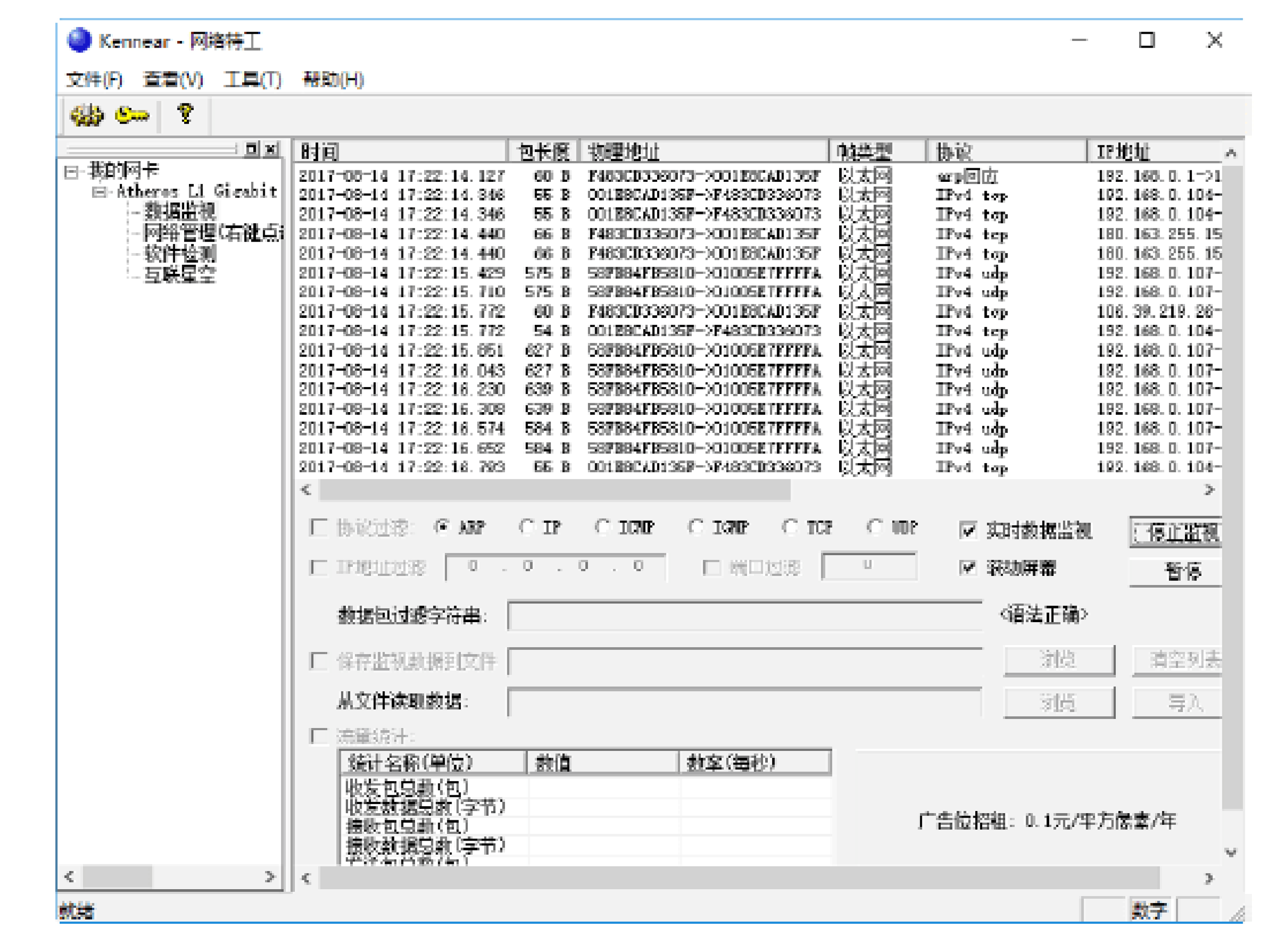
Step 01 下载并运行其中的“网络特工.exe”程序，即可打开“网络特工”主窗口，如下图所示。



Step 02 选择“工具”→“选项”选项，即可打开“选项”对话框，在其中设置相应的属性，如启动、全局热键等属性，如下图所示。



Step 03 在“网络特工”主窗口左边的列表中单击“数据监视”选项，即可打开“数据监视”窗口，如下图所示。在其中设置要监视的内容后，单击“开始监视”按钮，即可进行监视。

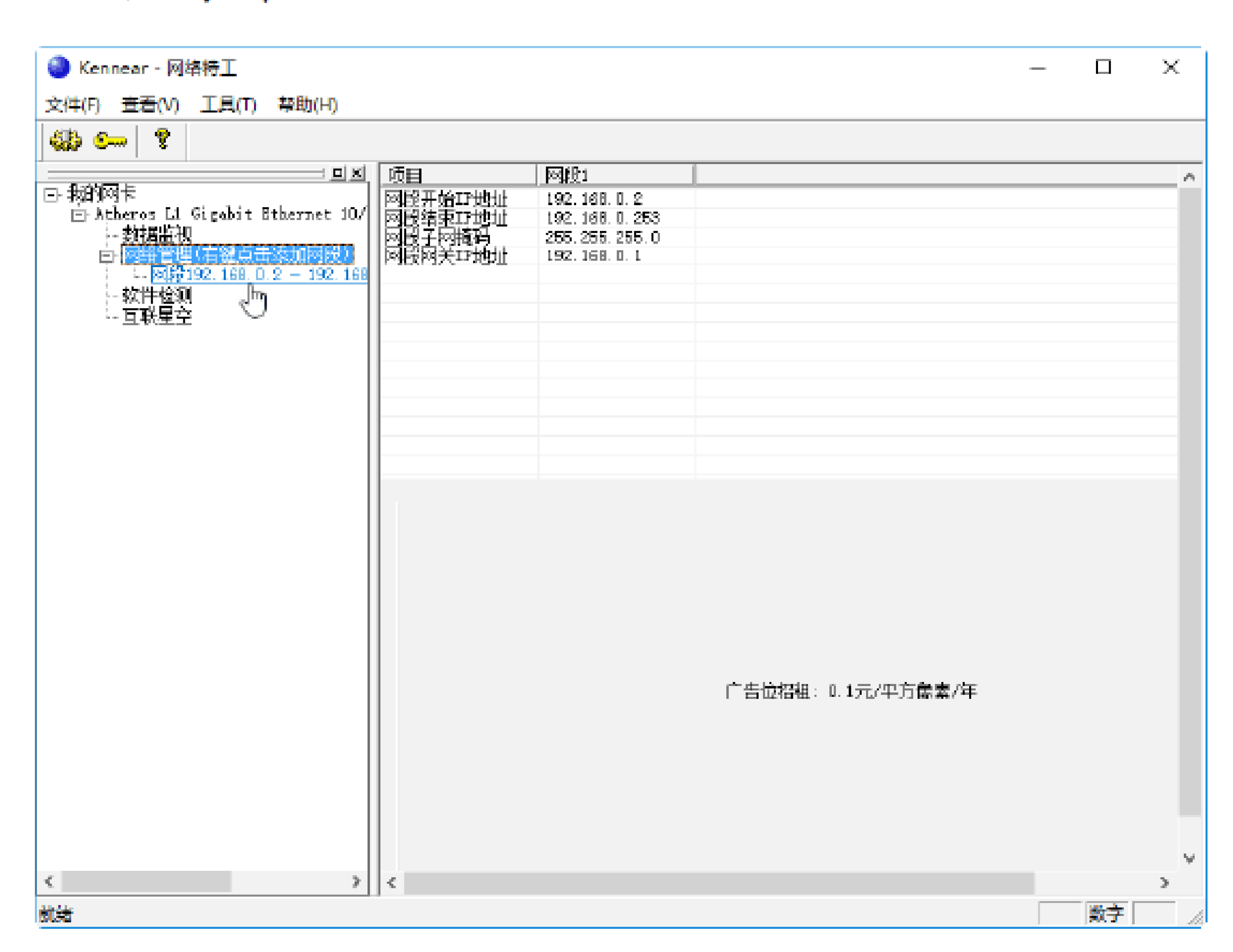




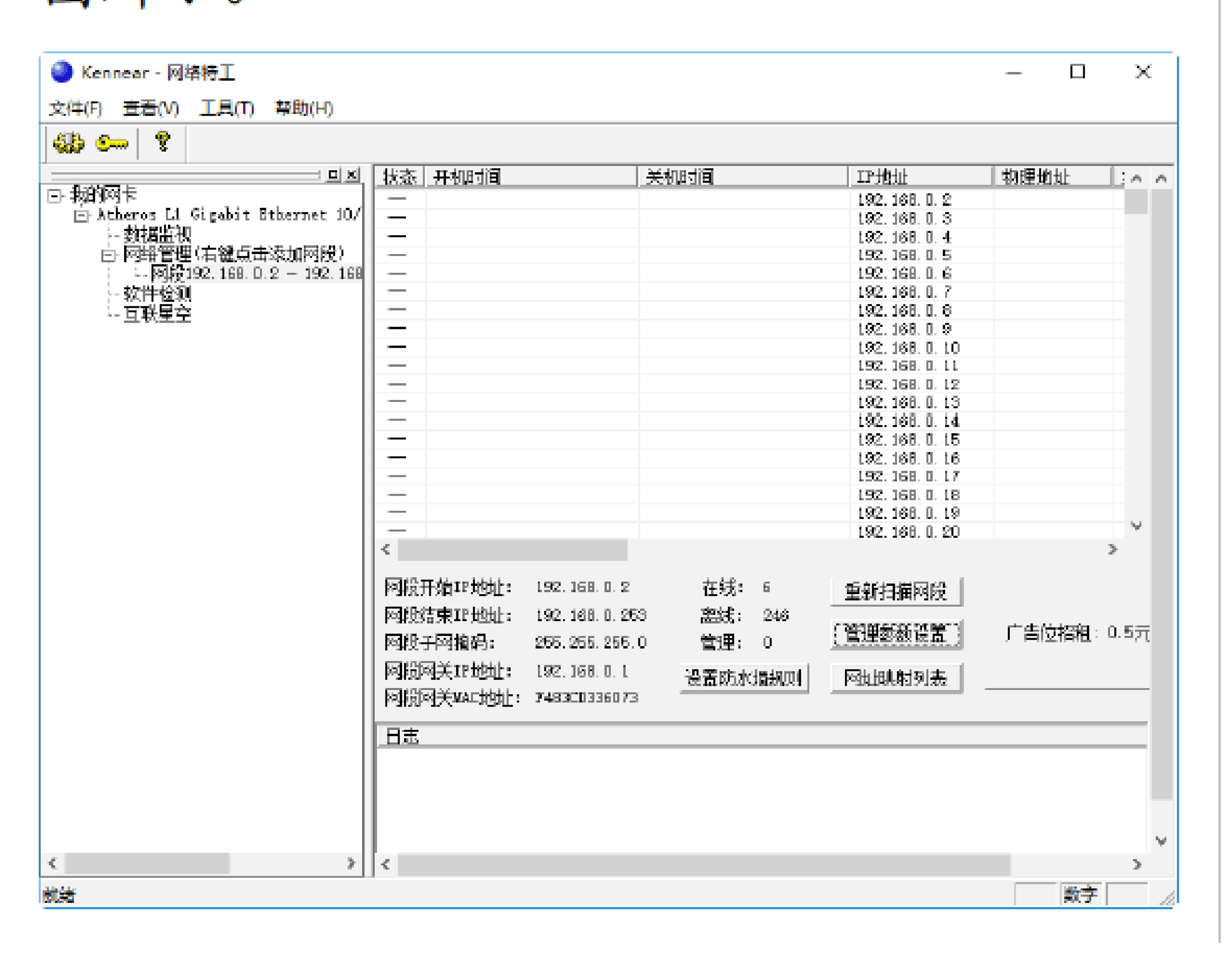
Step 04 在“网络特工”主窗口左边的列表中右击“网络管理”选项，在弹出的快捷菜单中选择“添加新网段”选项，即可打开“添加新网段”对话框，如下图所示。



Step 05 在设置网段的开始IP地址、结束IP地址、子网掩码、网关IP地址之后，单击OK按钮，即可在“网络特工”主窗口左边的“网络管理”选项中看到新添加的网段，如下图所示。



Step 06 双击该网段，即可在右边打开的窗口中，看到刚设置网段中所有的信息，如下图所示。



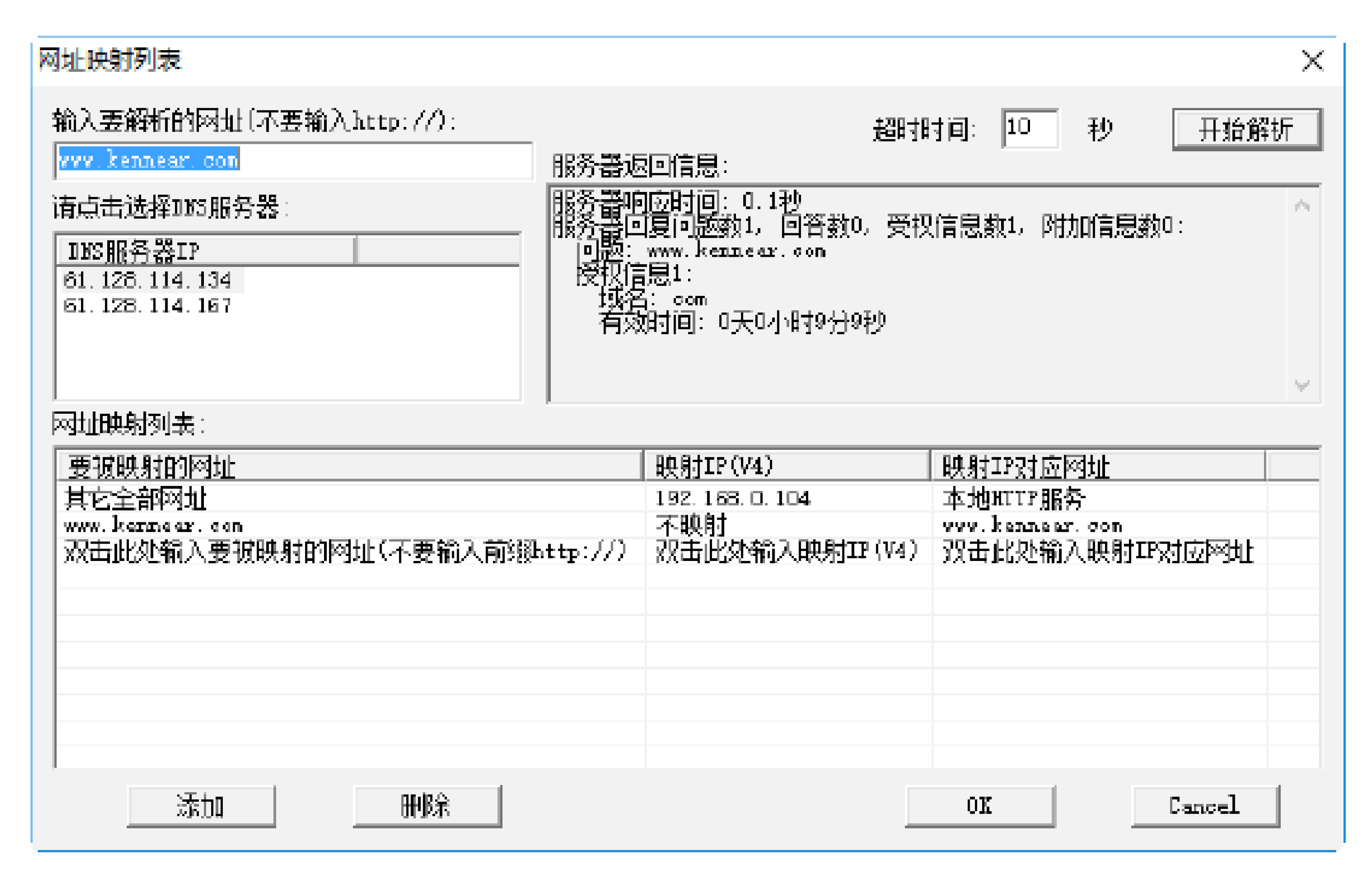
Step 07 单击其中的“管理参数设置”按钮，即可打开“网段参数设置”对话框，在其中对各个网络参数进行设置，如下图所示。



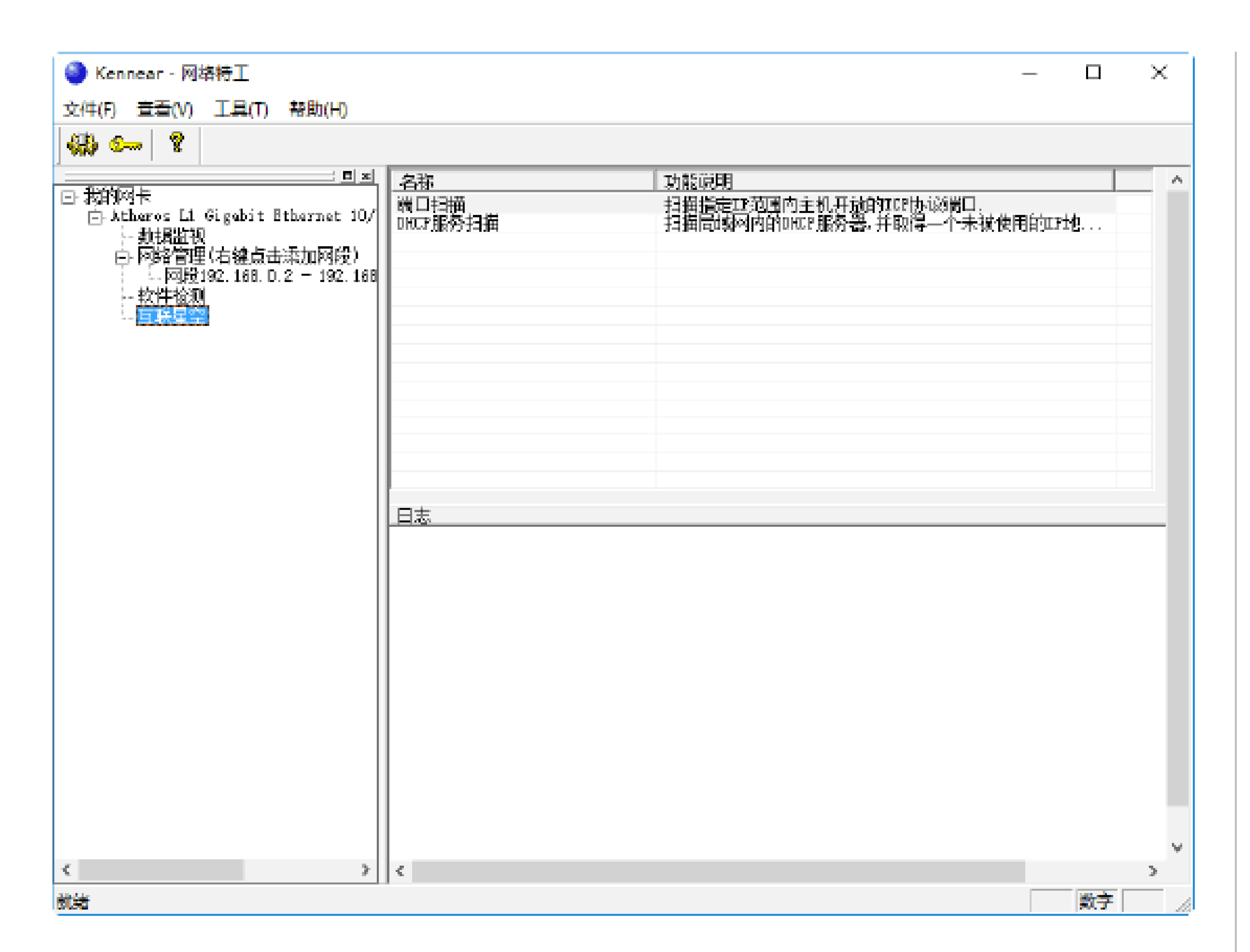
Step 08 单击“网址映射列表”按钮，即可打开“网址映射列表”对话框，如下图所示。



Step 09 在“DNS服务器IP”文本区域选中要解析的DNS服务器，单击“开始解析”按钮，即可对选中的DNS服务器进行解析，待解析完毕，即可看到该域名对应的主机地址等属性，如下图所示。



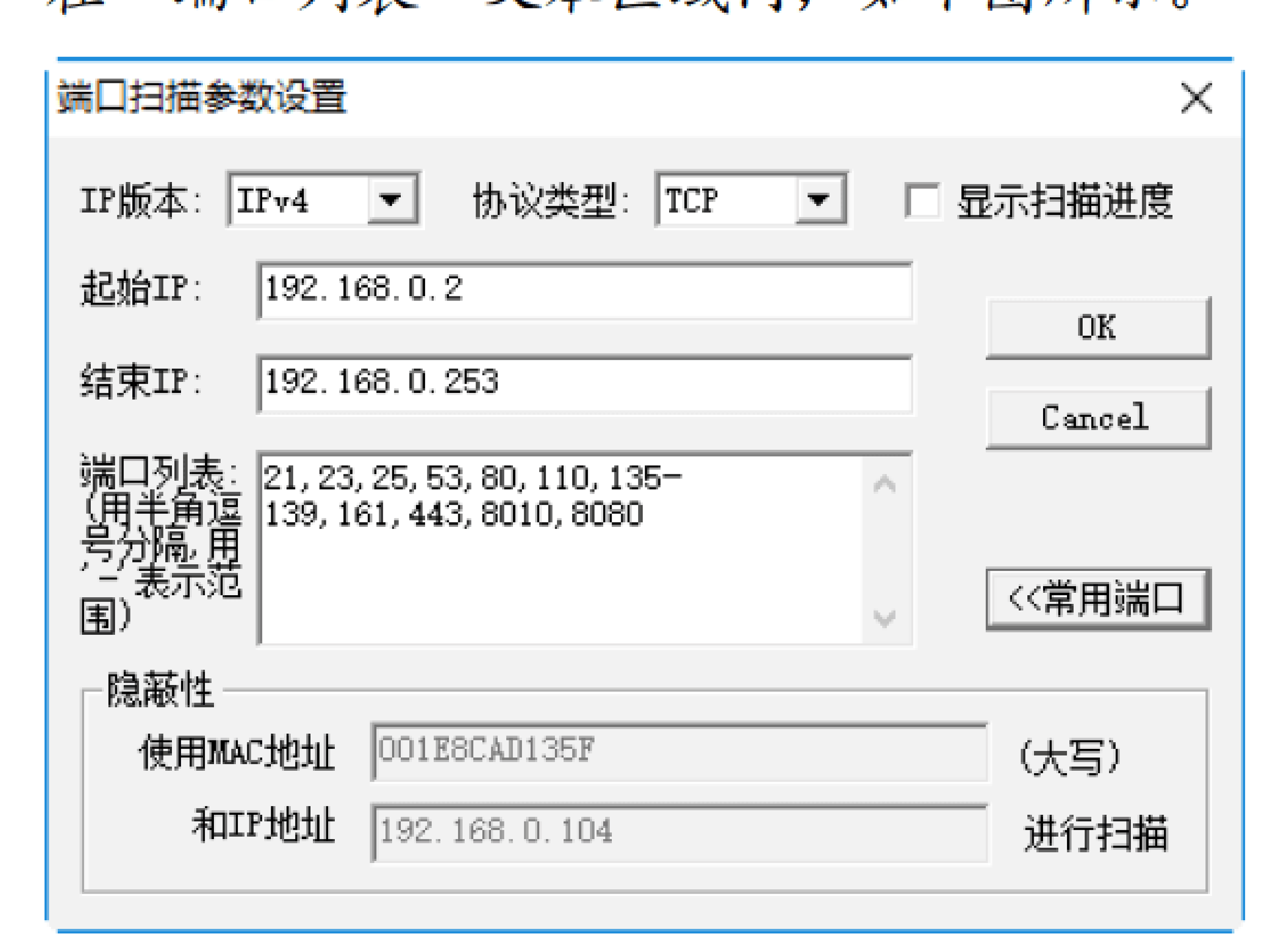
Step 10 在“网络特工”主窗口左边的列表中单击“互联星空”选项，即可打开“互联星空”窗口，在其中即可进行扫描端口和DHCP服务操作，如下图所示。



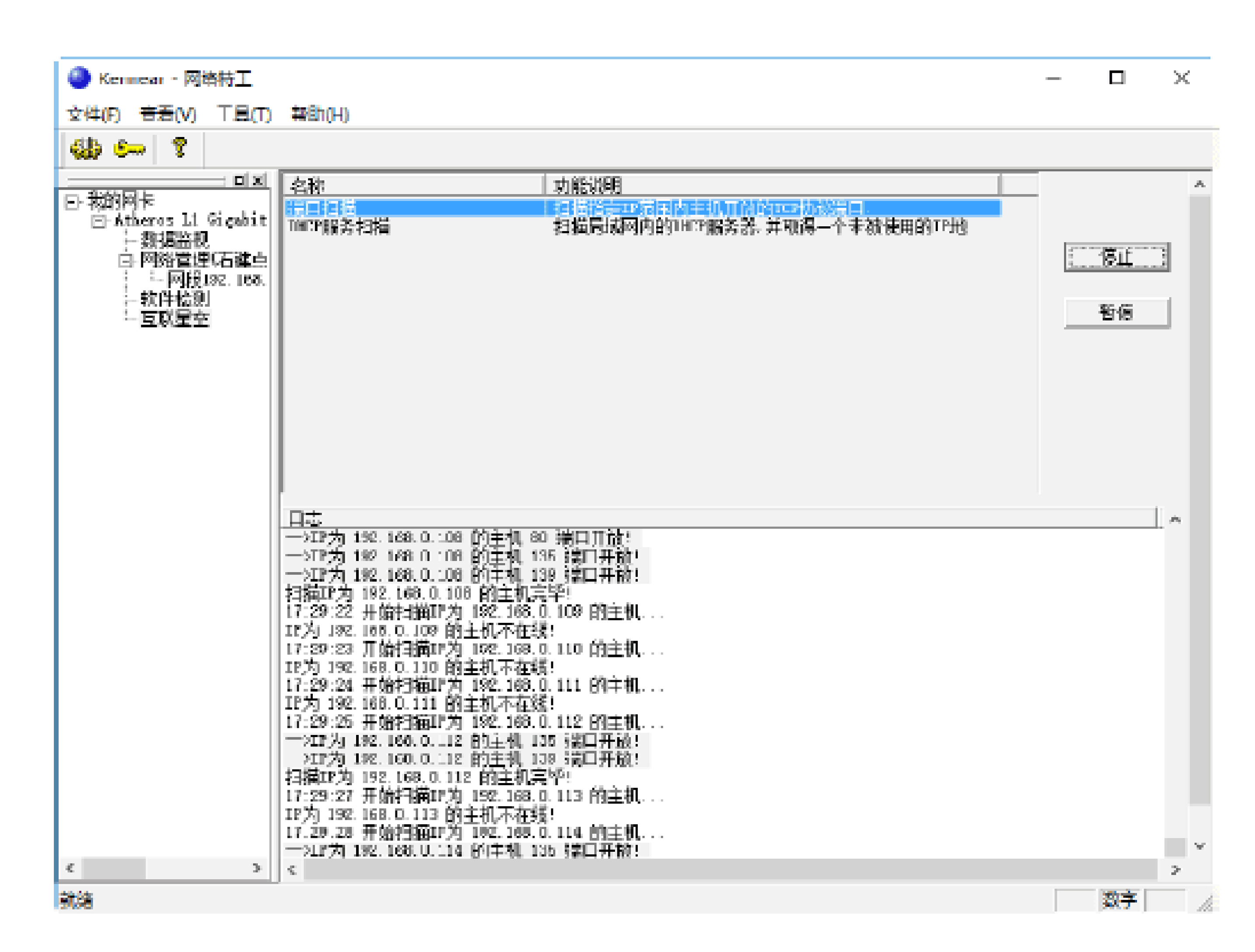
Step 11 在右边的列表中选择“端口扫描”选项，单击“开始”按钮，即可打开“端口扫描参数设置”对话框，如下图所示。



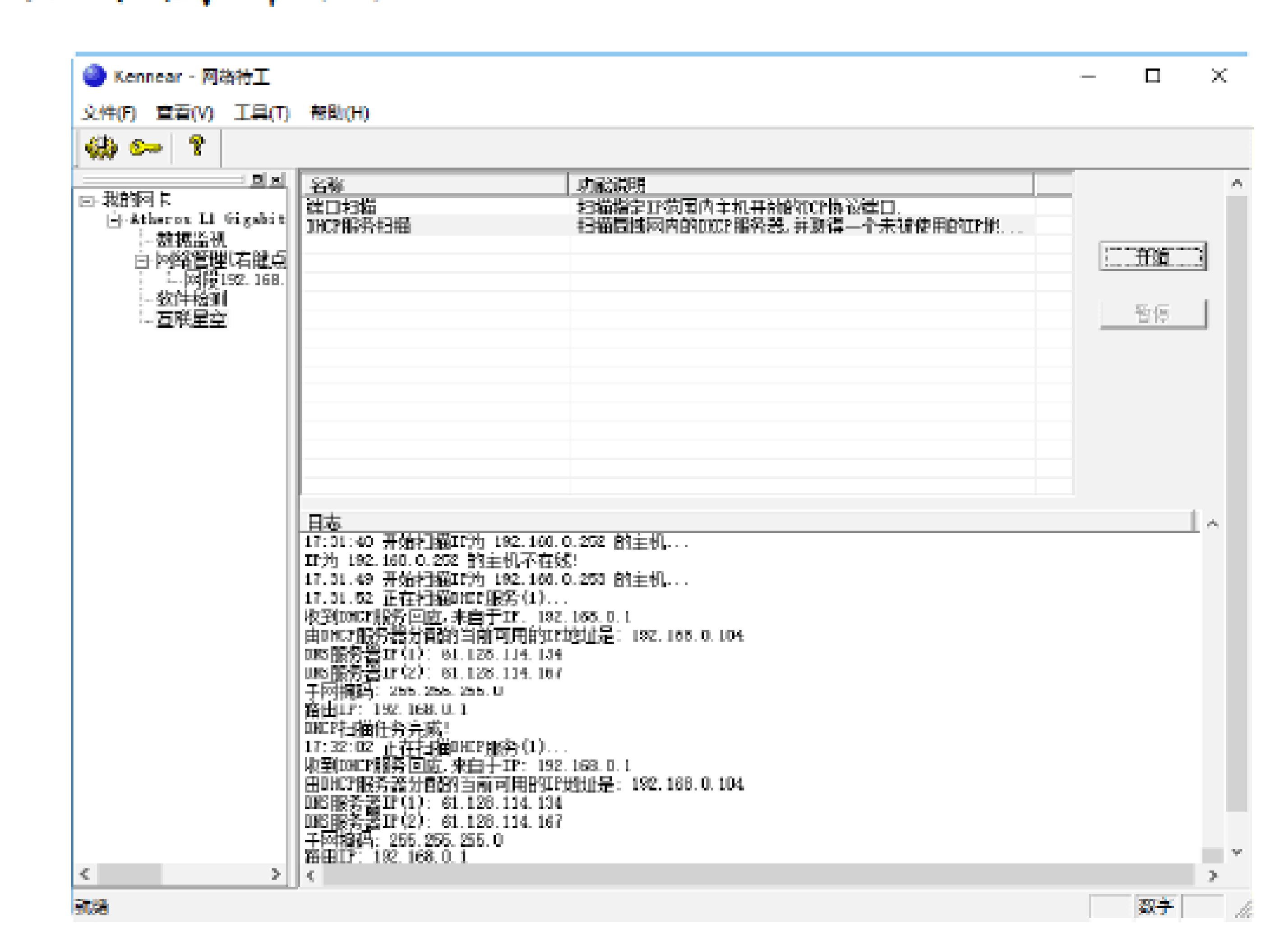
Step 12 在设置起始IP和结束IP之后，单击“常用端口”按钮，即可将常用的端口显示在“端口列表”文本区域内，如下图所示。



Step 13 单击OK按钮，即可进行扫描端口操作，在扫描的同时，将扫描结果显示在下面的“日志”列表框中，在其中即可看到各个主机开启的端口，如下图所示。



Step 14 在“互联星空”窗口右边的列表中选择“DHCP服务扫描”选项后，单击“开始”按钮，即可进行DHCP服务扫描操作，如下图所示。



实战6：局域网中的网络欺骗攻击



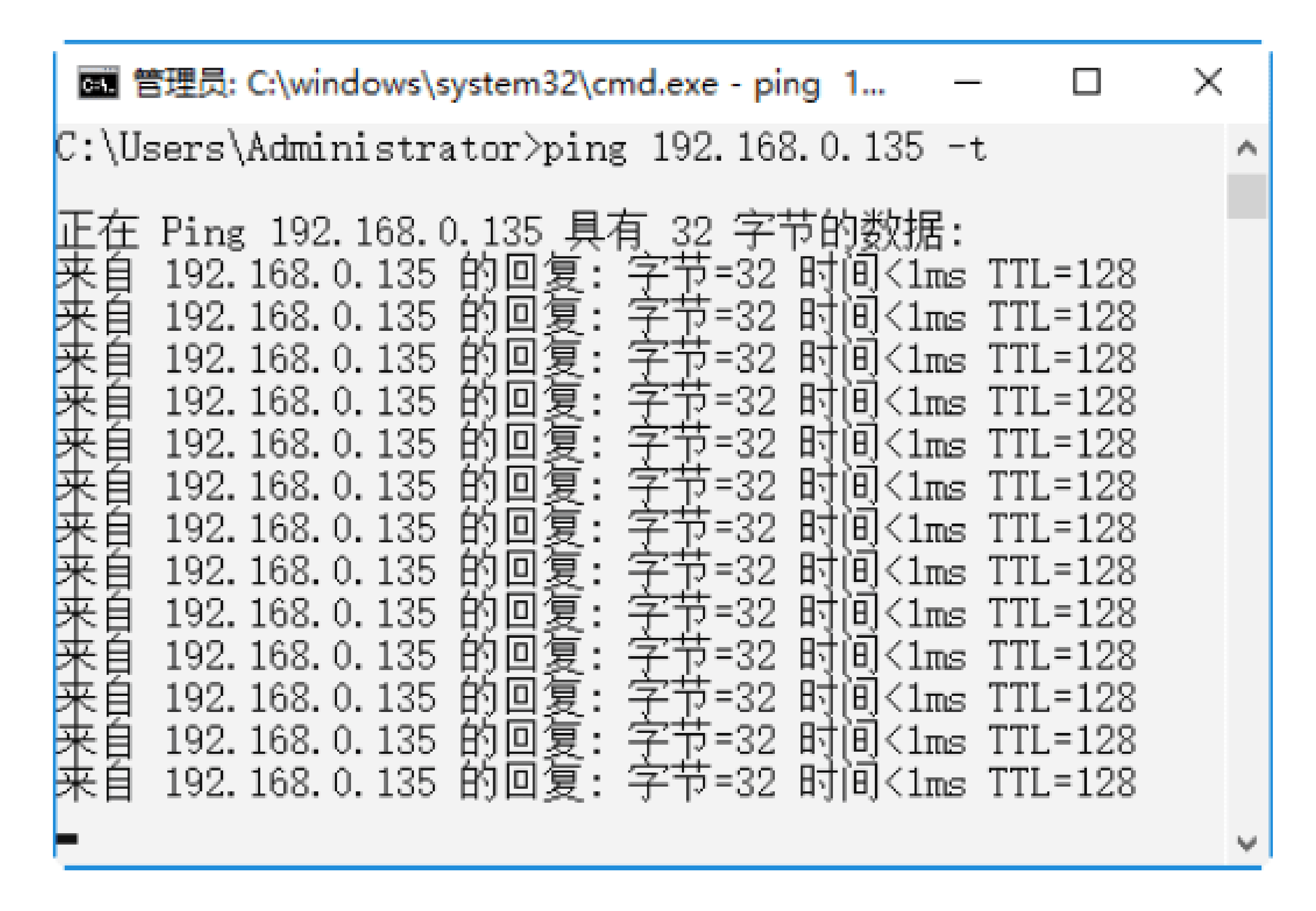
局域网终结者是用于攻击网吧中计算机的一款软件，其作用是构造虚假ARP数据包欺骗网络主机，使目标主机与网络断开。

使用局域网终结者欺骗网络主机的具体操作步骤如下。

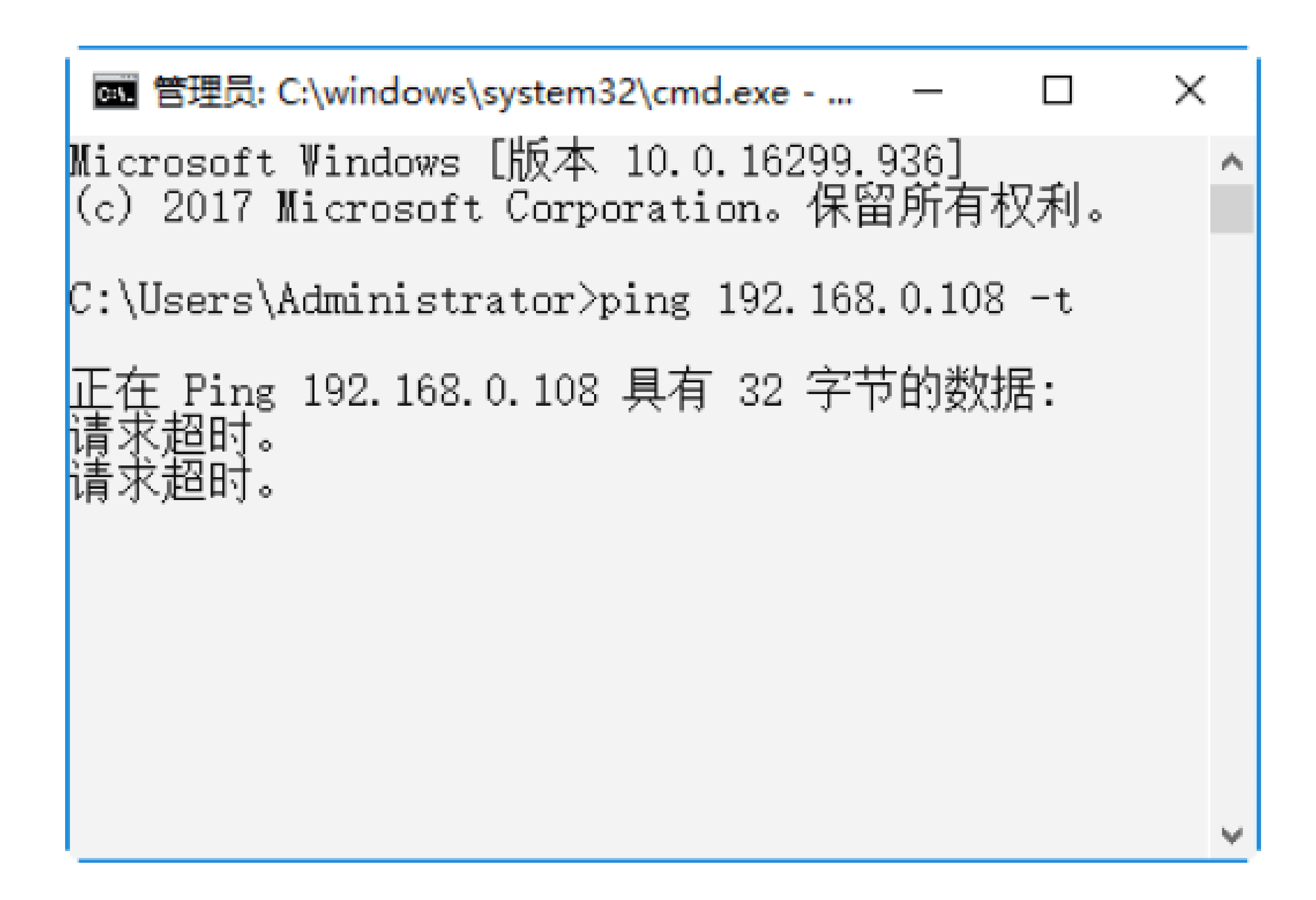
Step 01 在“命令提示符”窗口输入Ipconfig命令，按Enter键，即可查看本机的IP地址，如下图所示。



Step 02 在“命令提示符”窗口中输入“ping 192.168.0.135 -t”命令，按Enter键，即可检测本机与目标主机之间是否连通，如下图所示。如果出现相应的数据信息，则表示可以对该主机进行ARP欺骗攻击。

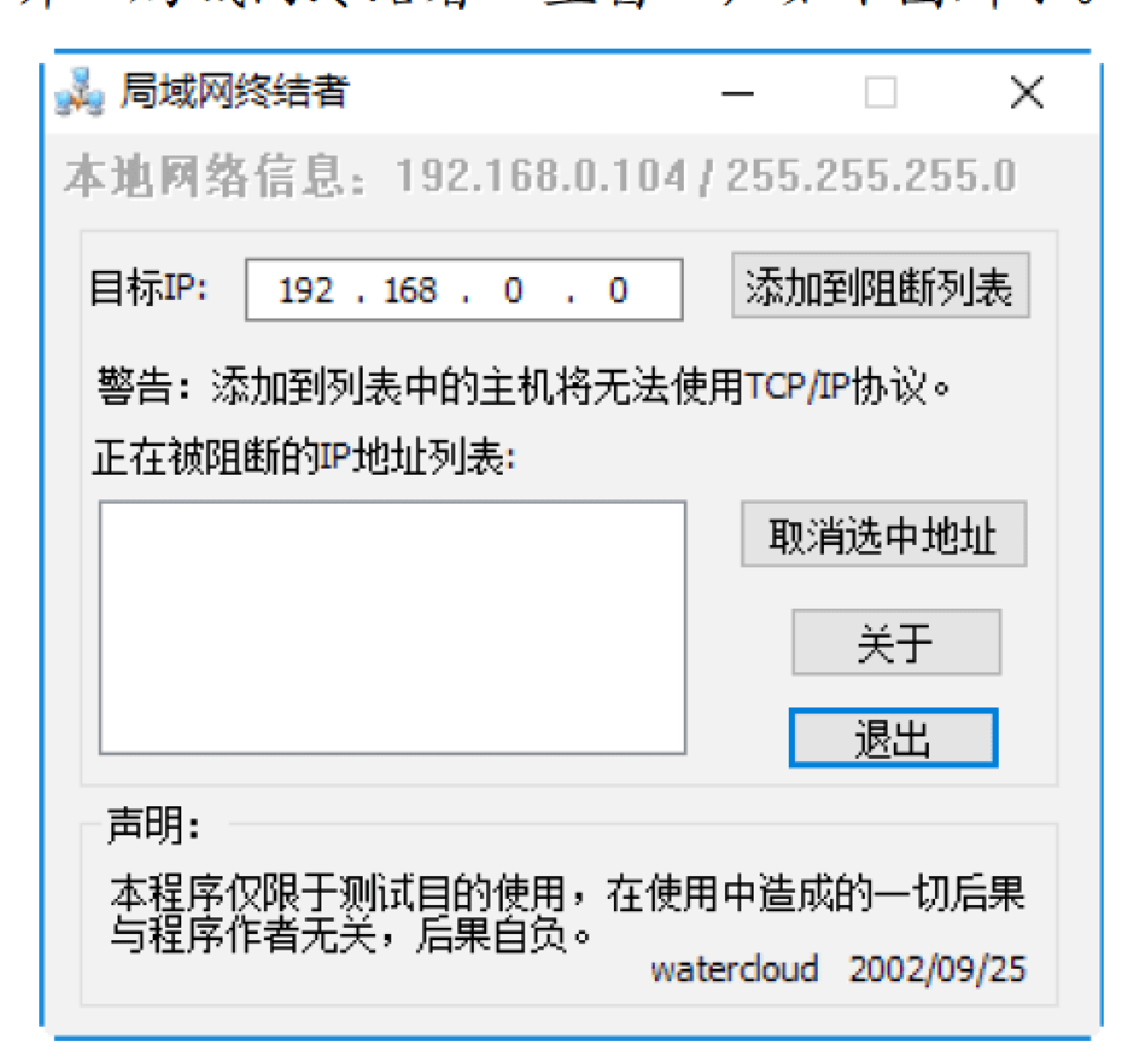


Step 03 如果出现“请求超时”提示信息，则说明对方已经启用防火墙，此时就无法对主机进行ARP欺骗攻击，如下图所示。

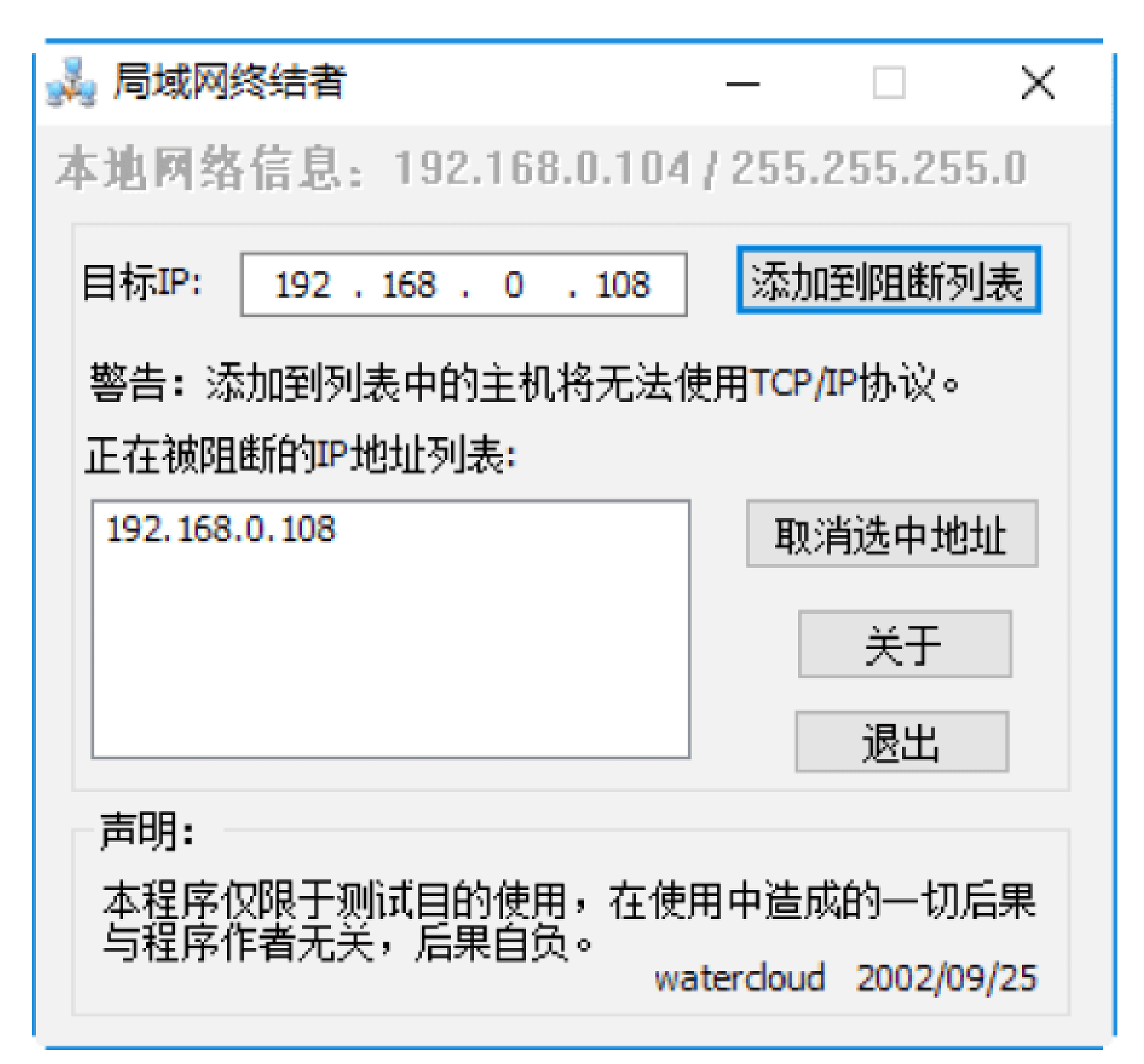




Step 04 运行“局域网终结者”主程序后，打开“局域网终结者”主窗口，如下图所示。



Step 05 在“目标IP”文本框中输入要控制目标主机的IP地址，然后单击“添加到阻断列表”按钮，即可将该IP地址添加到阻断列表中，如下图所示。如果此时目标主机中出现IP冲突的提示信息，则表示攻击成功。



9.4 局域网安全的防护

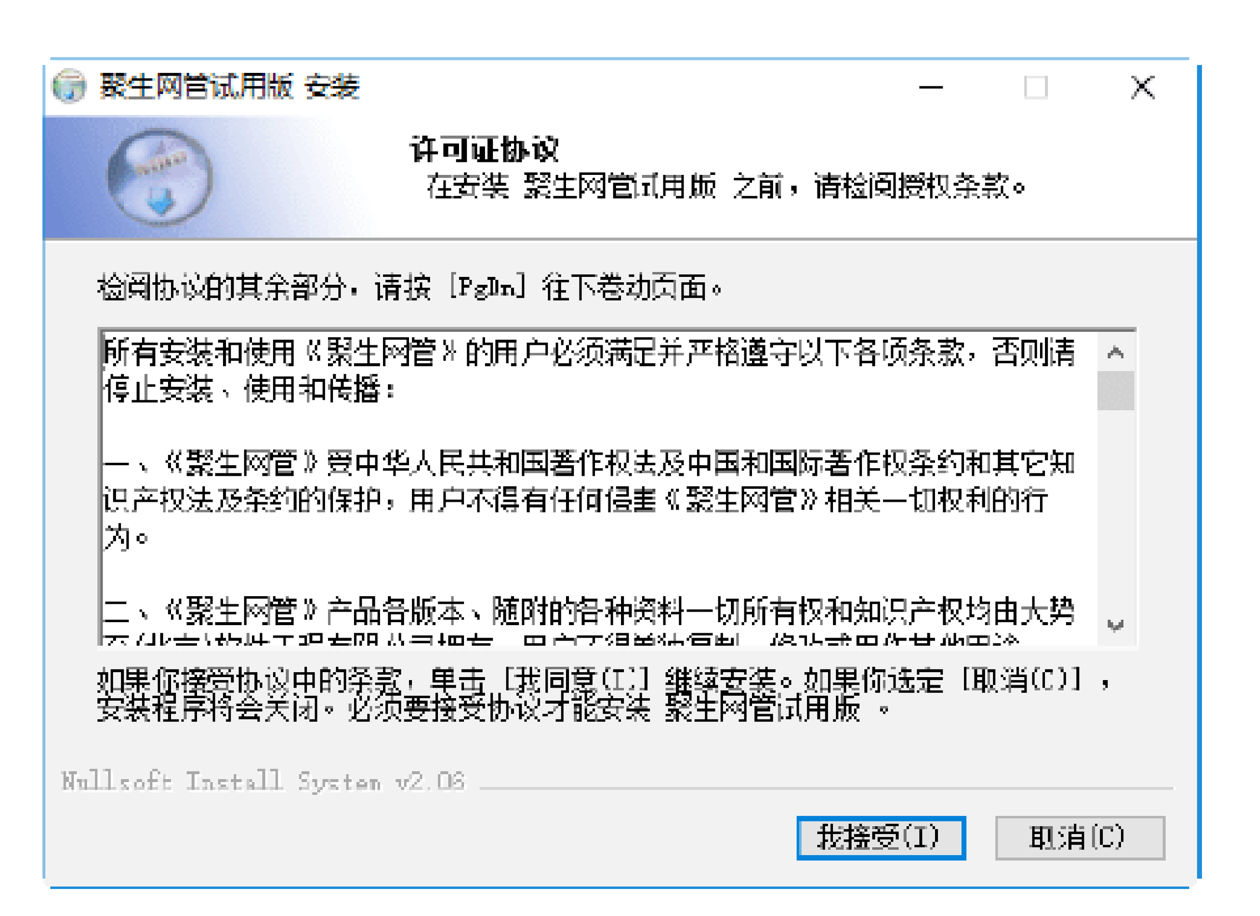
面对黑客针对局域网的种种攻击，局域网管理者可以使用局域网安全辅助工具来对整个局域网进行防护。本节介绍几款经典的局域网辅助工具，以帮助大家维护局域网，从而保护局域网的安全。

实战7：使用“聚生网管”管理局域网

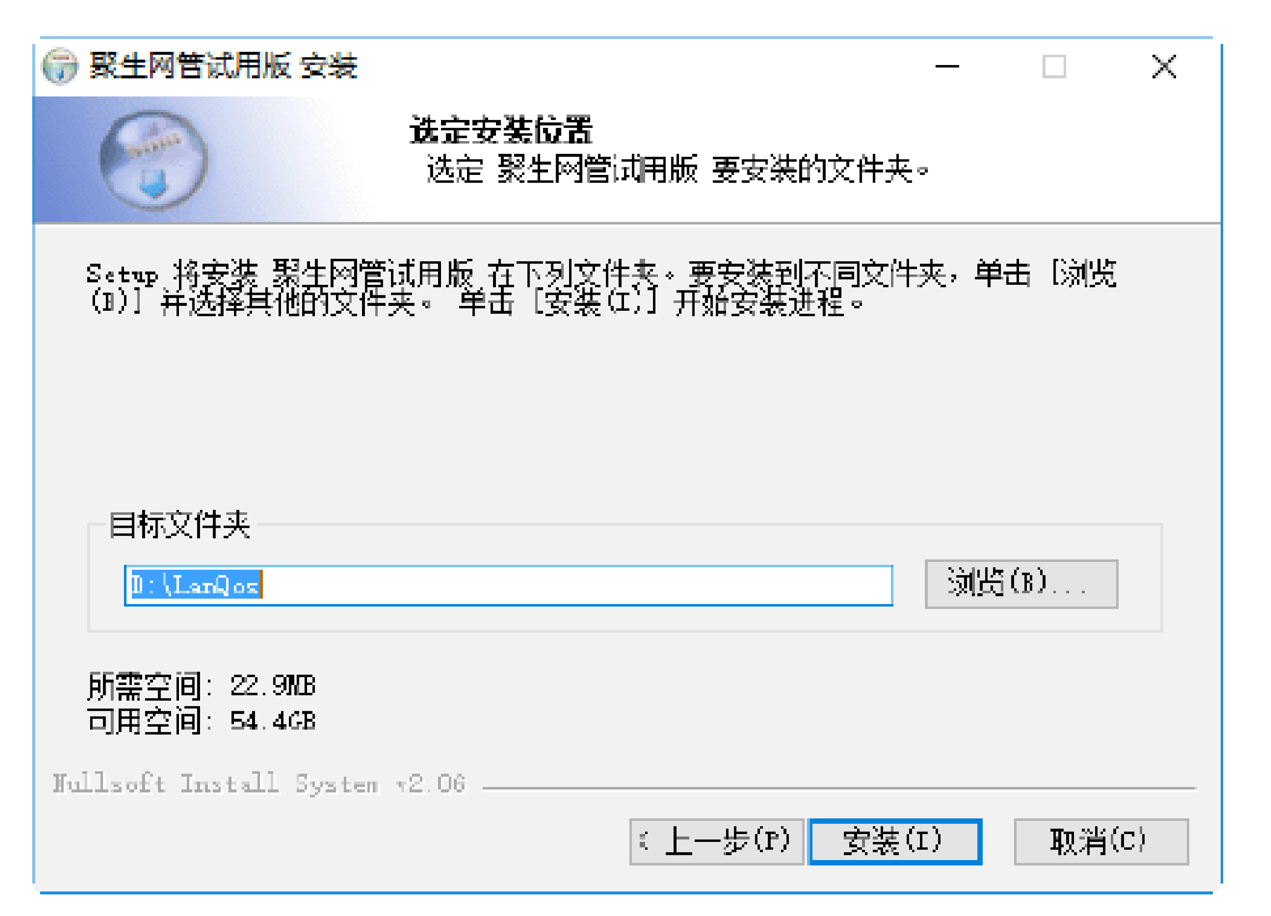
“聚生网管”是一套优秀的网络监控软件，用户只需要在局域网的任意一台计算机上安装该工具，就可以控制整个局域网的P2P下载、各种聊天工具、股票软件、游戏软件等，使得网管人员可以在一台控制机上就可以控制任意一台局域网主机，从而极大地提高工作效率。

1. 安装“聚生网管”

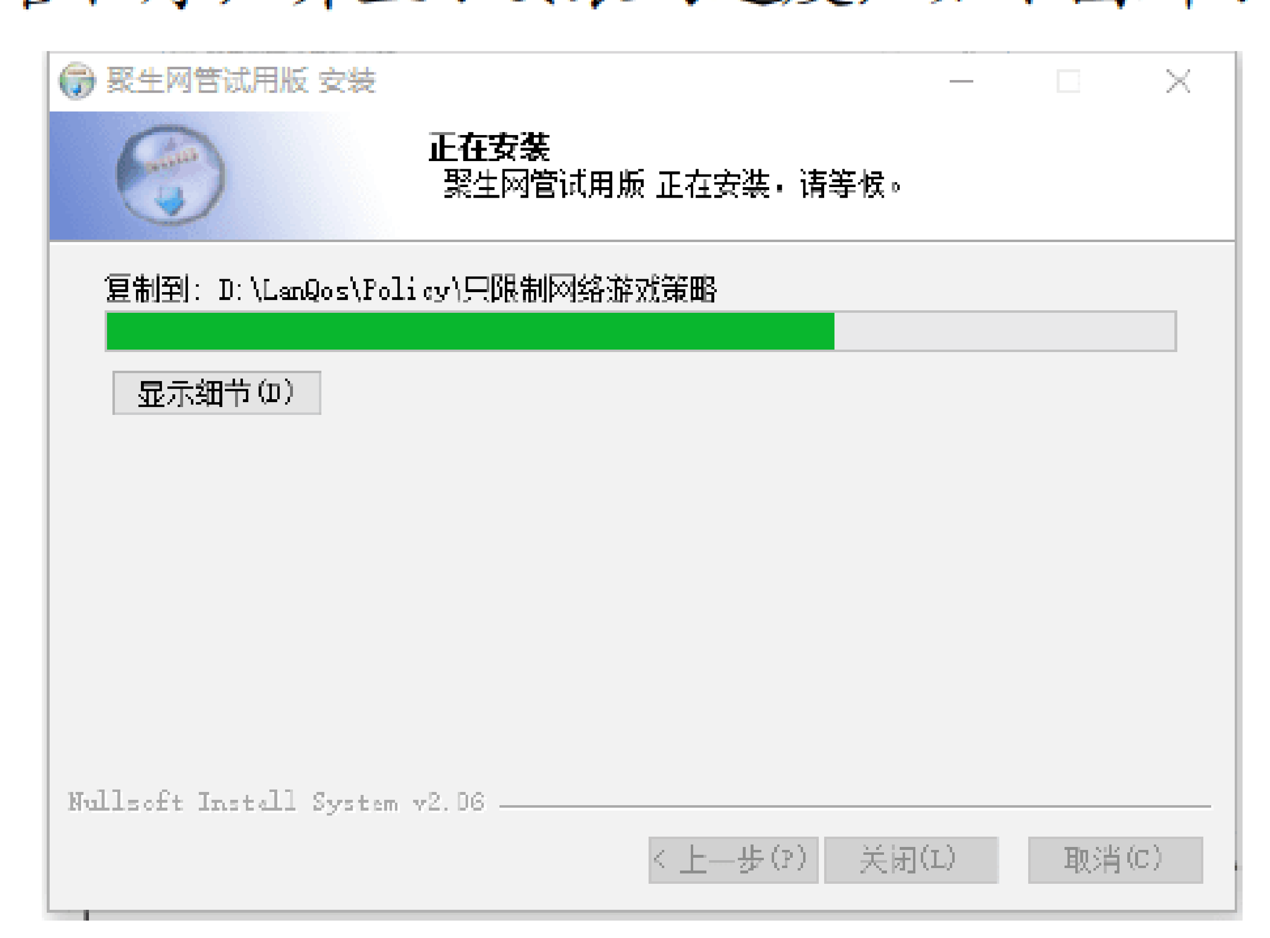
Step 01 双击下载的“聚生网管”安装程序，即可打开“许可证协议”对话框，在其中可以查看软件许可证协议信息，如下图所示。



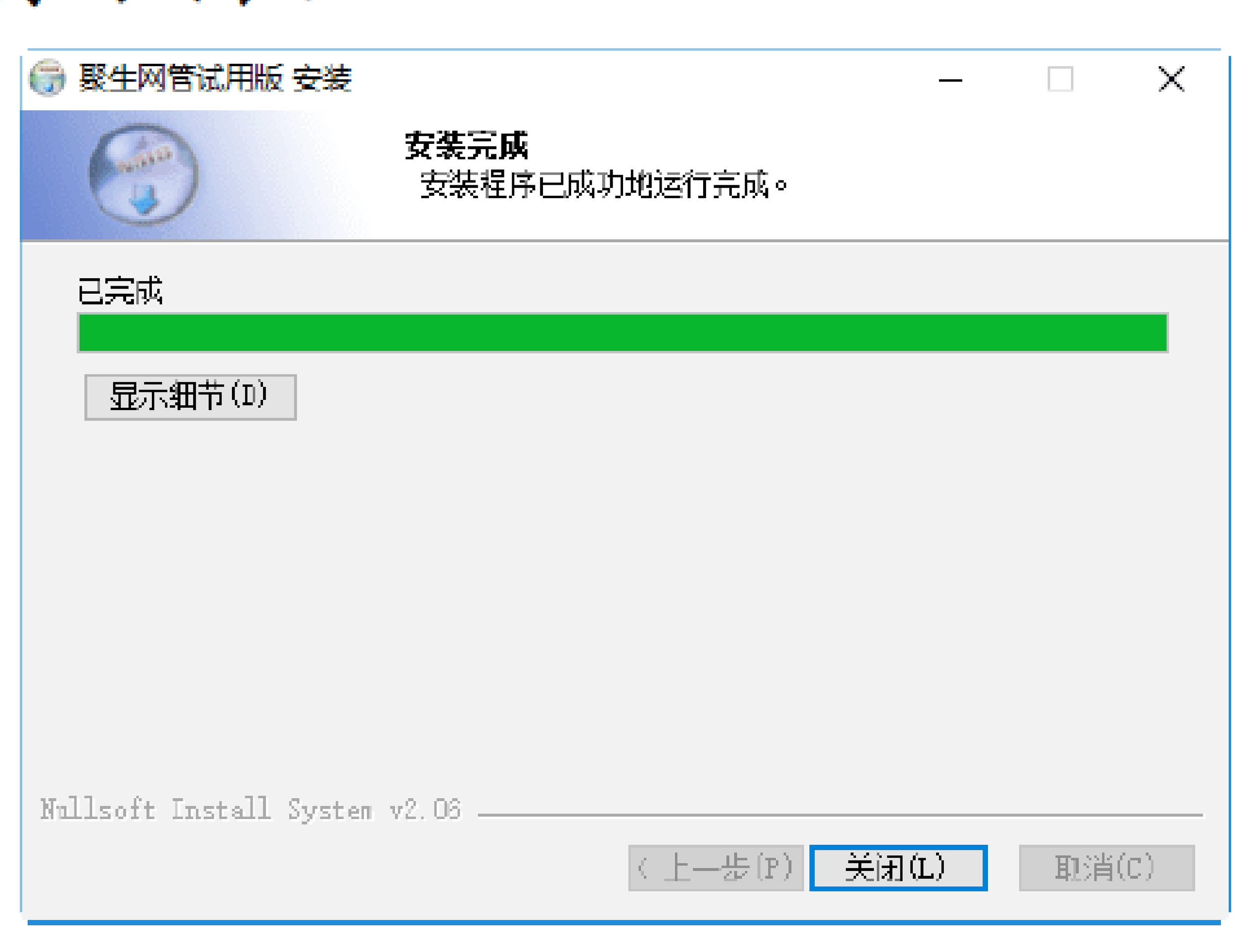
Step 02 单击“我接受”按钮，打开“选定安装位置”界面，在其中设置程序的安装目标文件夹，如下图所示。



Step 03 单击“安装”按钮，即可开始安装聚生网管程序，并显示安装的进度，如下图所示。



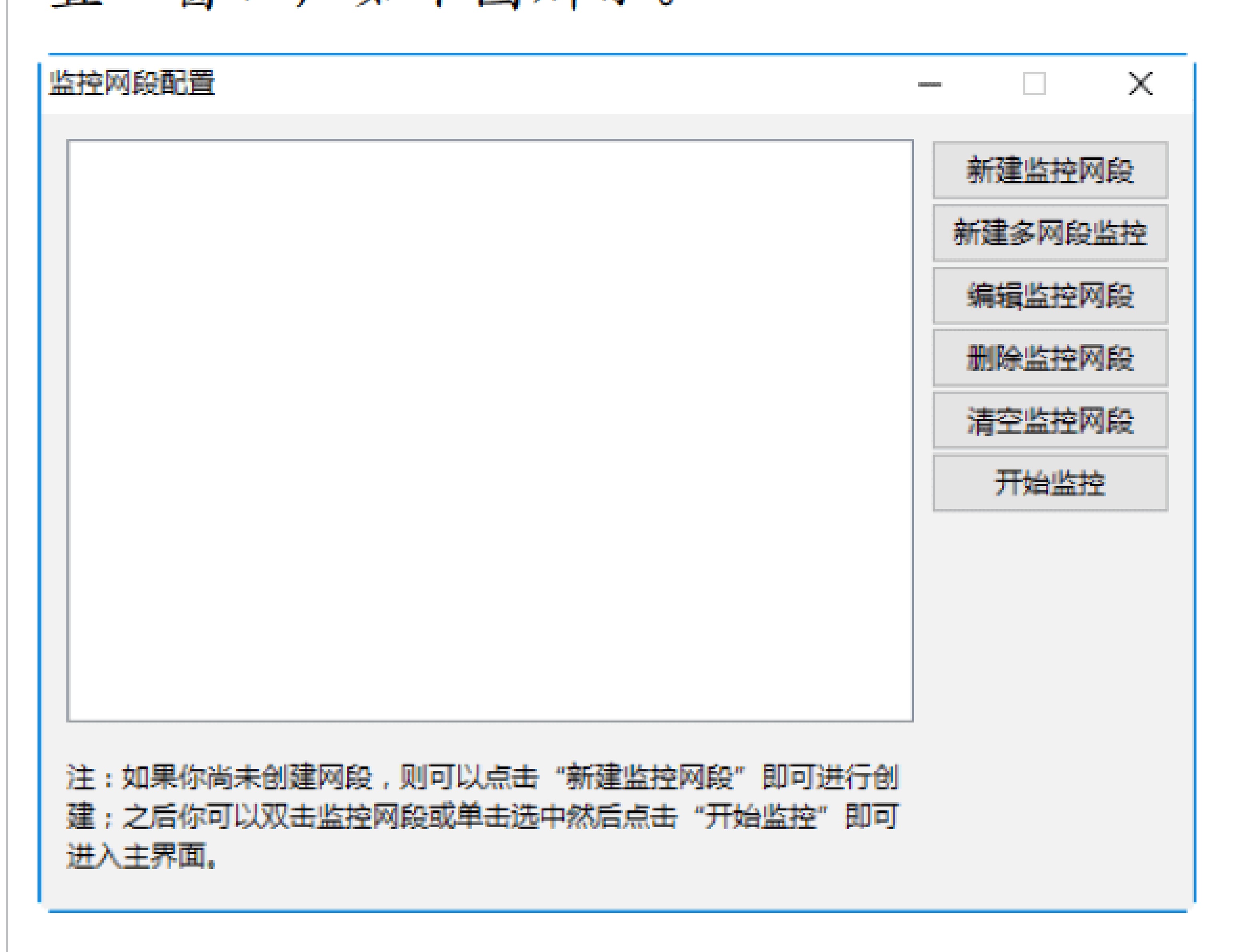
Step 04 安装完成后，弹出“安装完成”界面，如下图所示，单击“关闭”按钮，完成程序的安装。



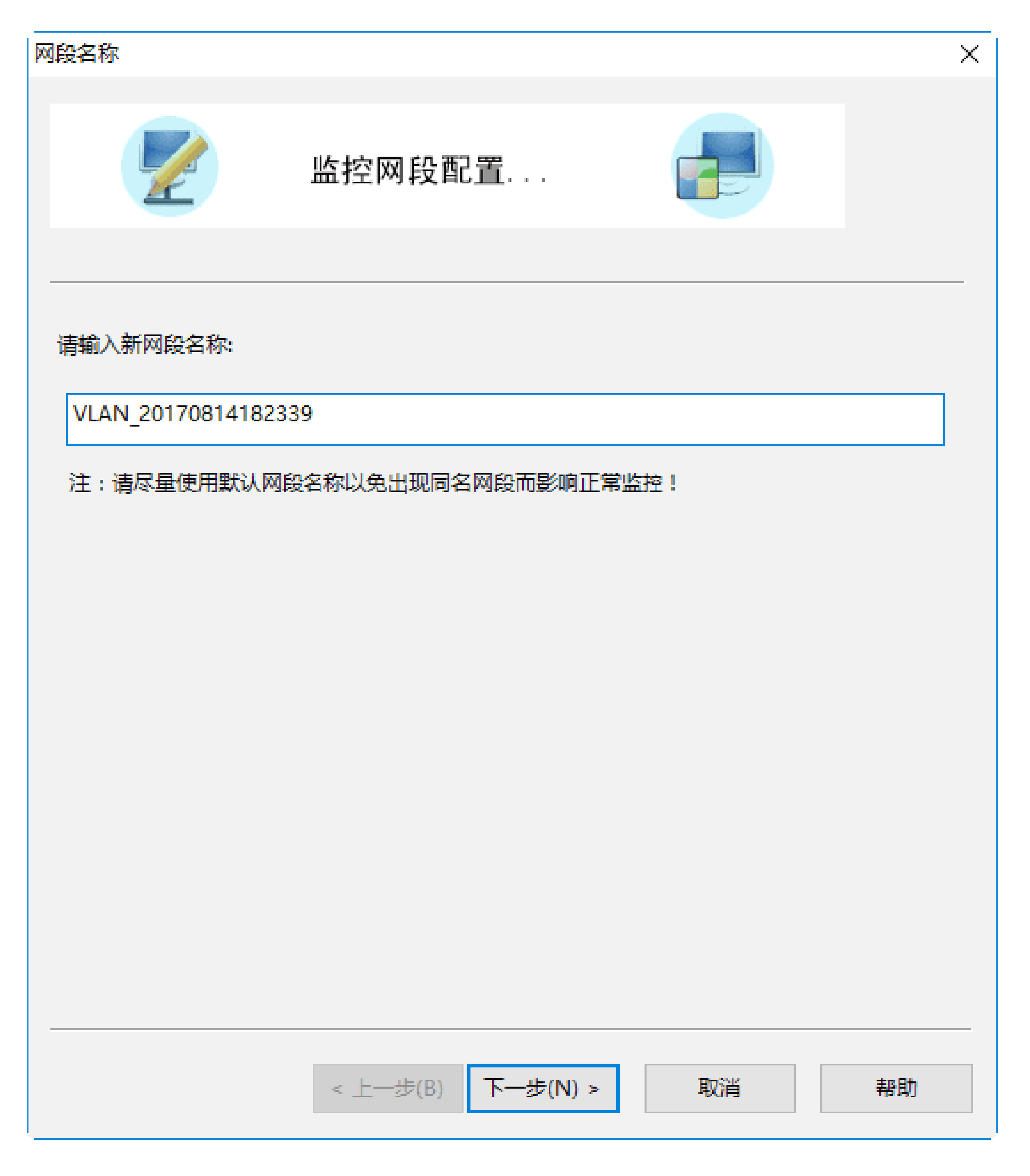
2.“聚生网管”的配置

在使用“聚生网管”工具之前，需要先对其进行配置。配置聚生网管的具体操作步骤如下。

Step 01 选择“开始”→“所有应用”→“聚生网管”选项，即可打开“监控网段配置”窗口，如下图所示。



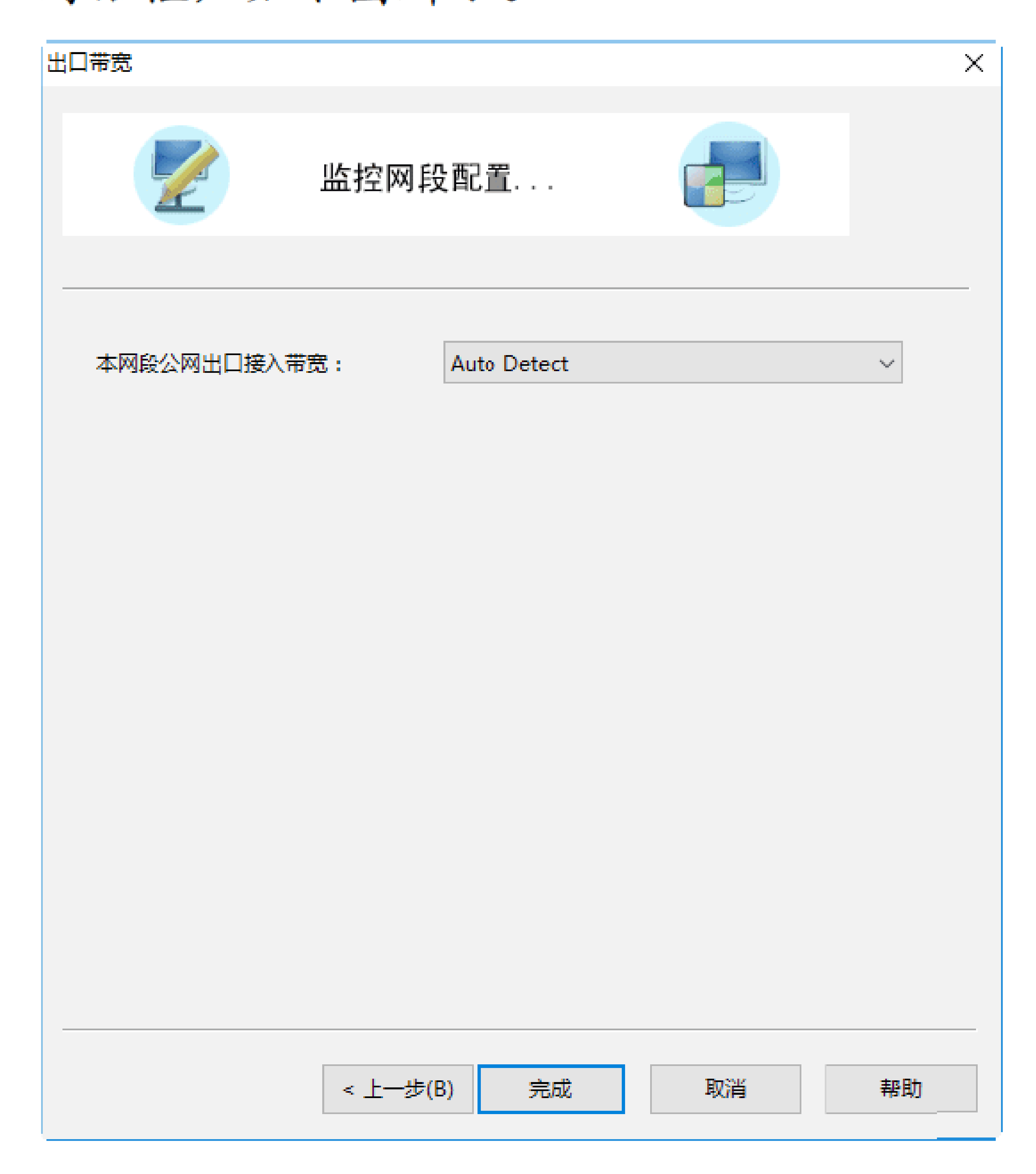
Step 02 在进行监控之前，需要添加要监控的网段，单击“新建监控网段”按钮，即可打开“网段名称”对话框，如下图所示。



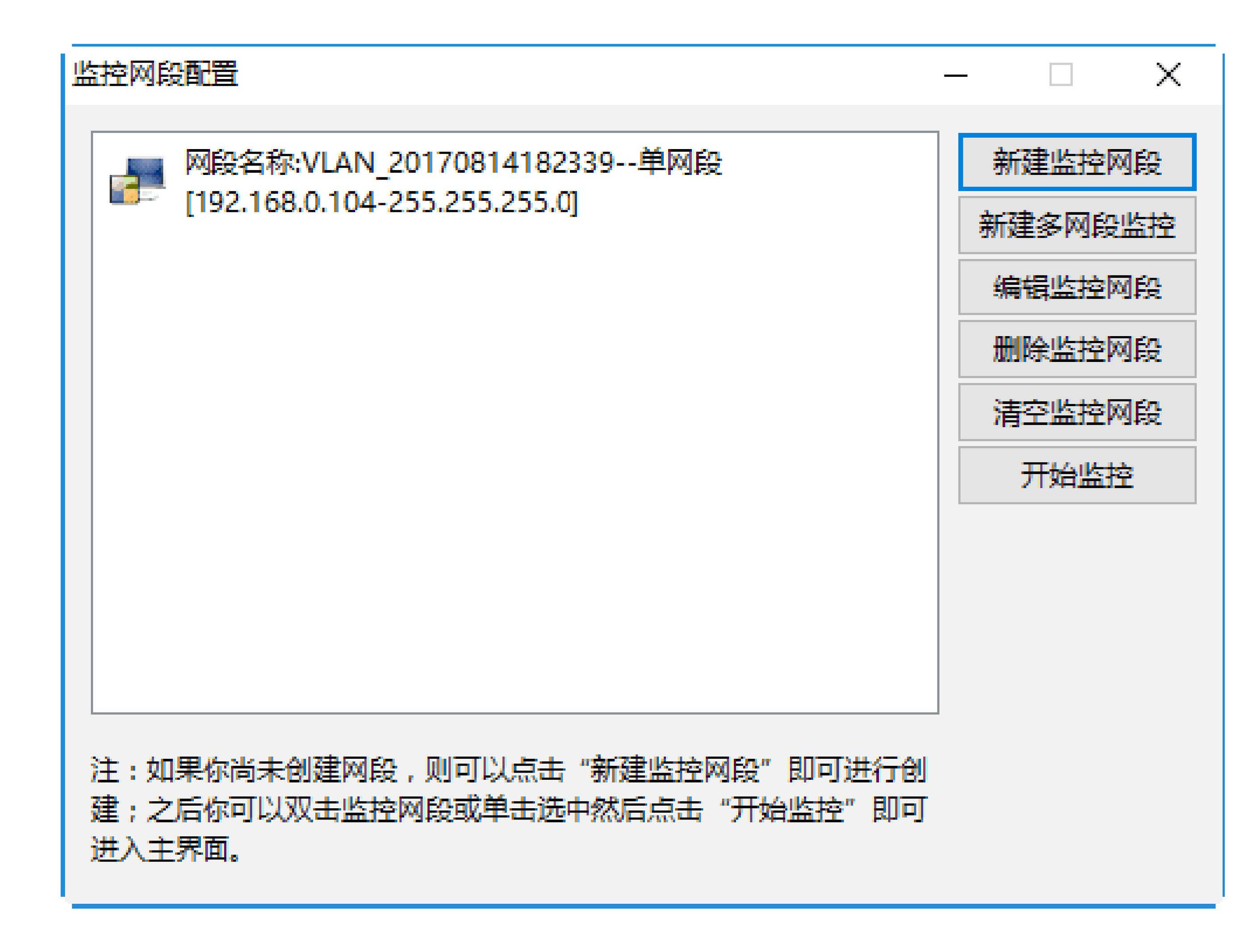
Step 03 在“请输入新网段名称”下方的文本框中输入网段的名称之后，单击“下一步”按钮，即可打开“选择网卡”对话框，如下图所示。



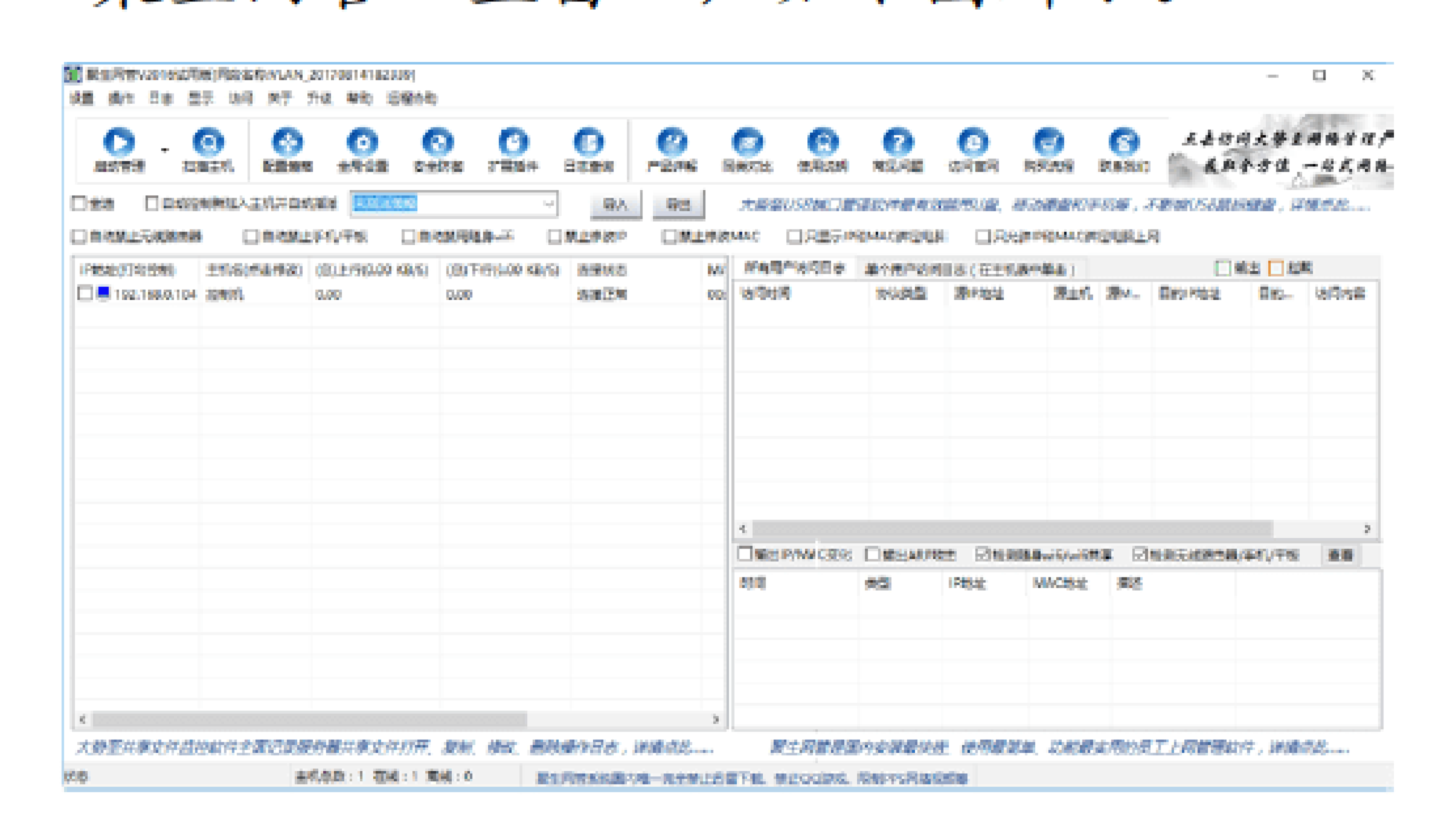
Step 04 为该网段选择对应的网卡后，单击“下一步”按钮，即可打开“出口带宽”对话框，如下图所示。



Step 05 在“本网段公网出口接入带宽”右侧的下拉列表中选择“Auto Detect（自动检测）”选项，单击“完成”按钮，将会返回到“监控网段配置”对话框，在其中即可看到所配置的监控网段信息，如下图所示。



Step 06 当确定所配置的监控网段信息准确无误后，单击“开始监控”按钮，即可打开“聚生网管”主窗口，如下图所示。

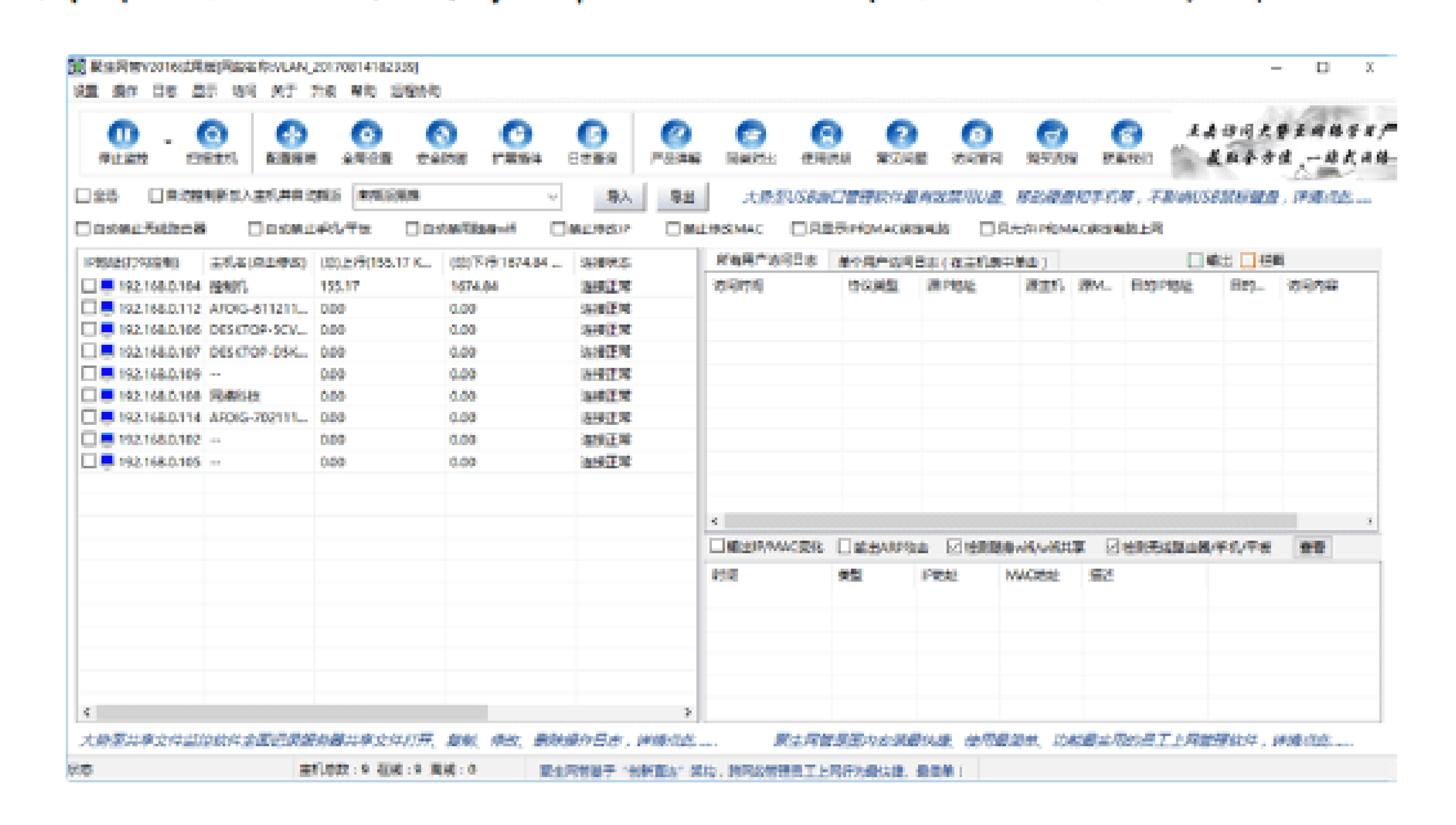


提示：用户可以根据需要建立多个网段。如果想监控第二个网段，再次打开一个聚生网管的窗口，从中选择想要建立的第二个网段，然后单击“开始监控”按钮即可。

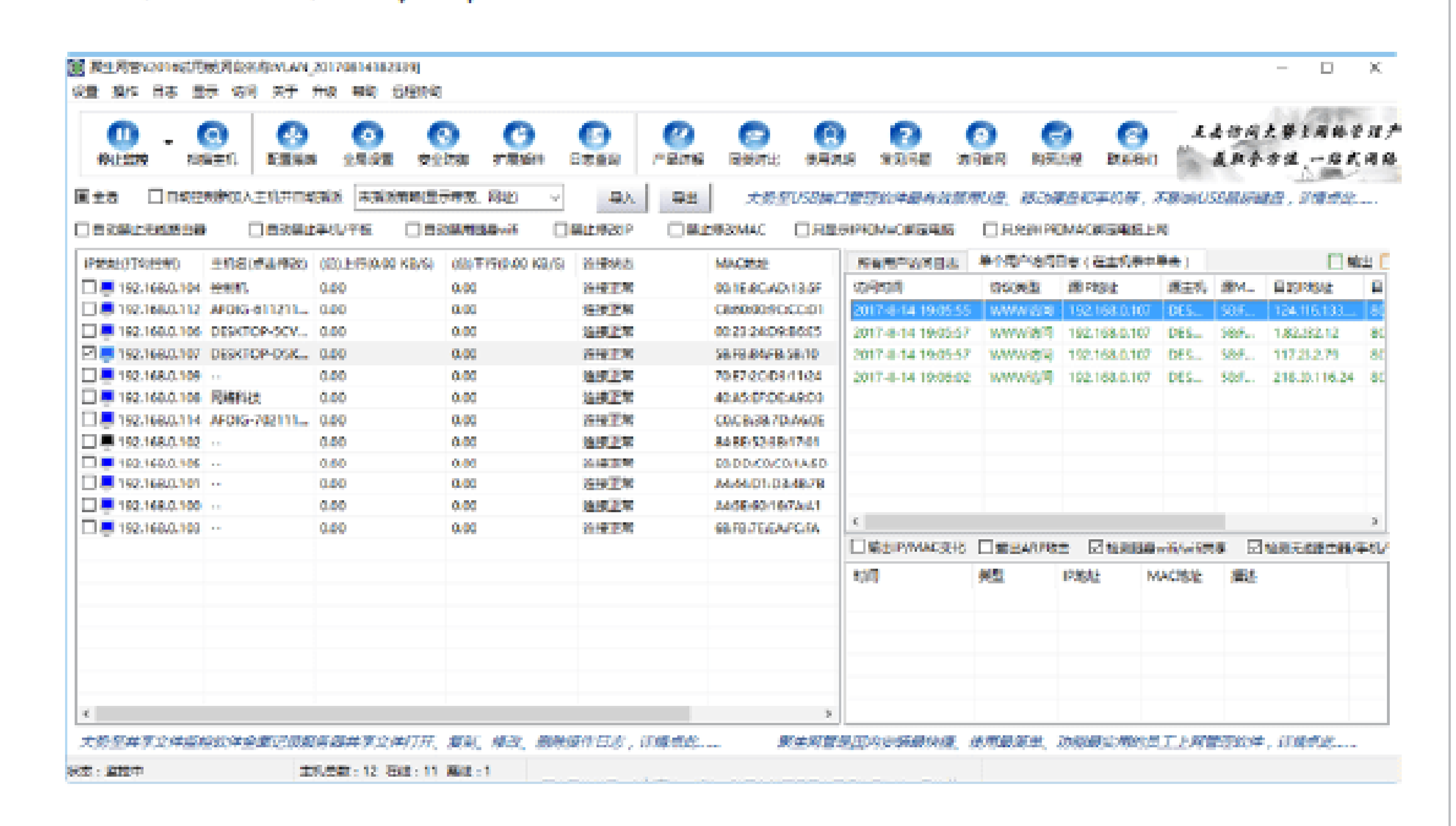
3.“聚生网管”的使用

在配置完聚生网管要监控的网段后，就可以利用该工具对整个局域网进行管理。具体操作步骤如下。

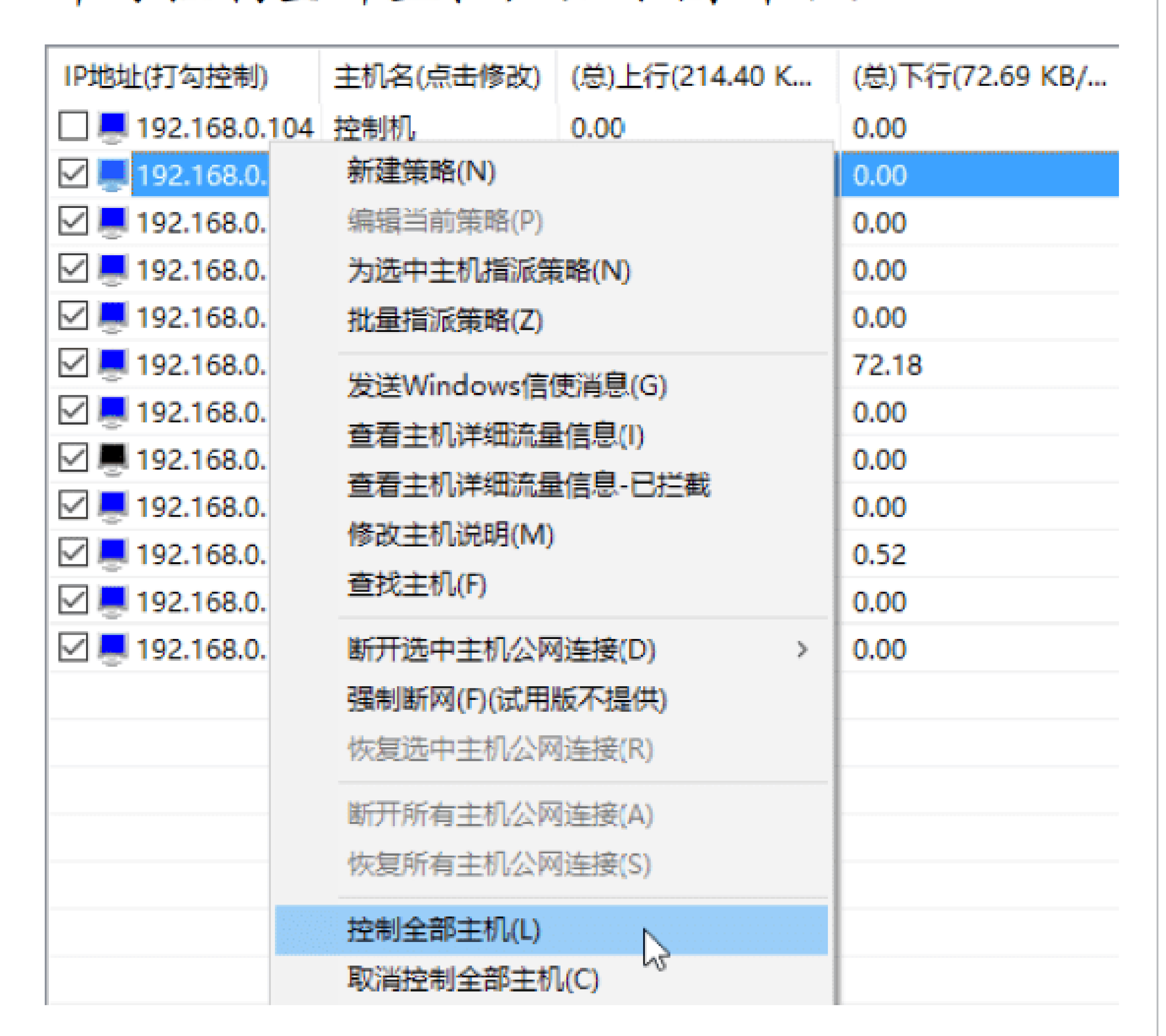
Step 01 在“聚生网管”主窗口中，单击“启动管理”按钮，即可扫描到所有在线主机，并在下方的列表中显示出来，如下图所示。



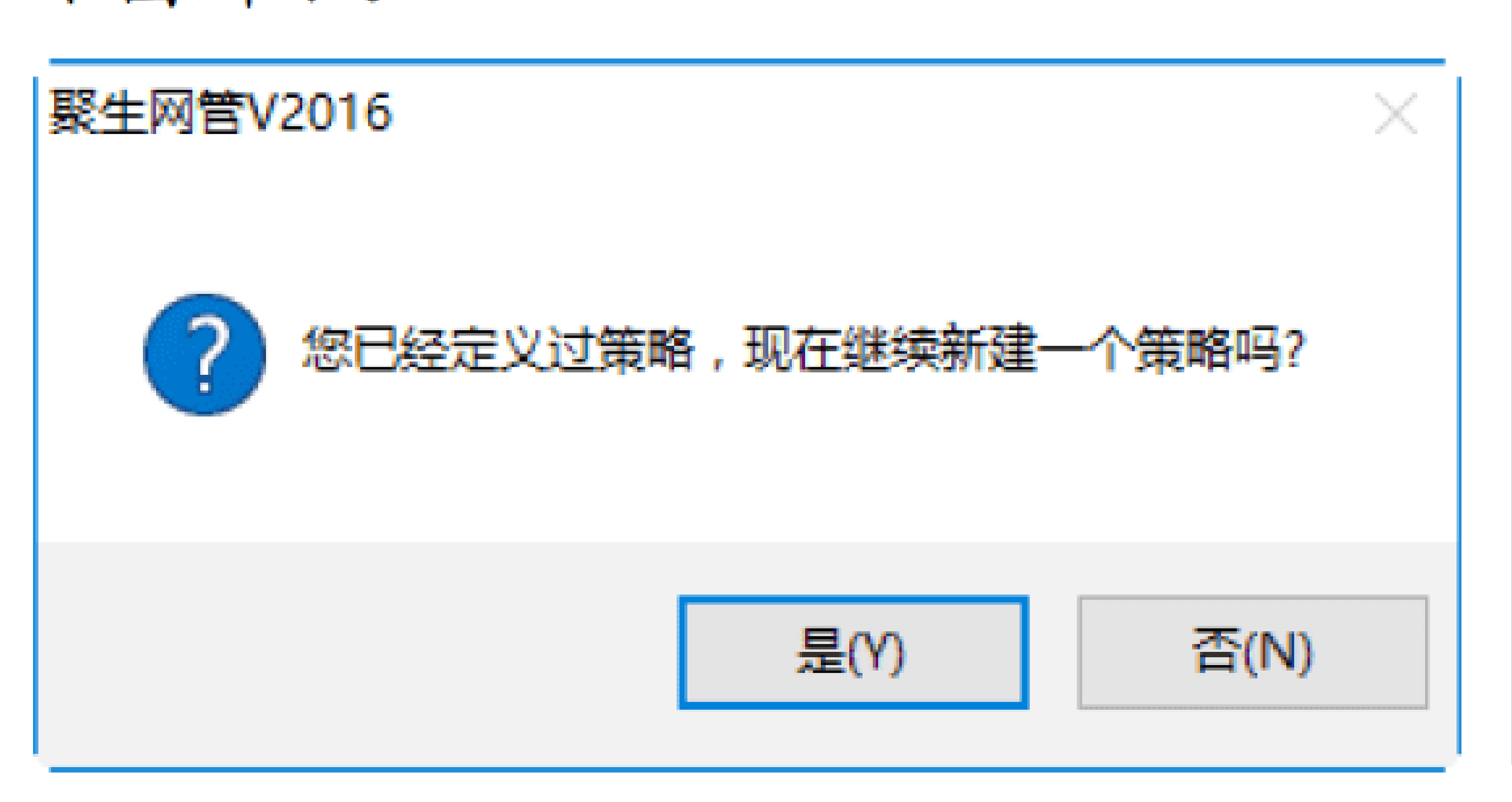
Step 02 选中主机前面的复选框，即可开始控制并显示计算机宽带、上网网址或拦截日志等信息；取消选中，则所有控制全部失效，如下图所示。



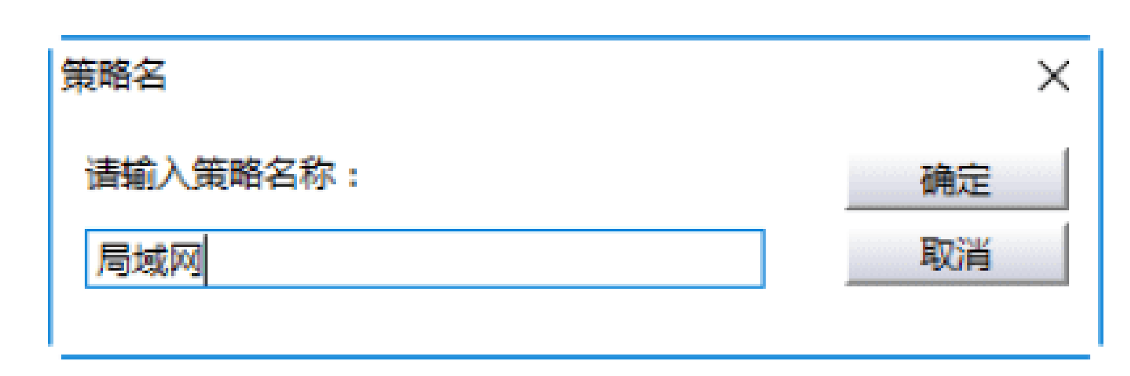
Step 03 在主机列表中，右击鼠标，在弹出的快捷菜单中选择“控制全部主机”选项，即可控制全部主机，如下图所示。



Step 04 虽然可以控制全部主机，但只是让用户查看带宽，并没有对主机进行其他的控制。如果想启用各种控制（如下载、聊天等），只需要双击某台主机信息，即可弹出“您已经定义过策略，现在继续新建一个策略吗？”提示框，如下图所示。



Step 05 若要新建策略，则需要单击“是”按钮，即可打开“策略名”对话框，在“请输入策略名称”文本框中输入一个策略的名称，如“局域网”，如下图所示。



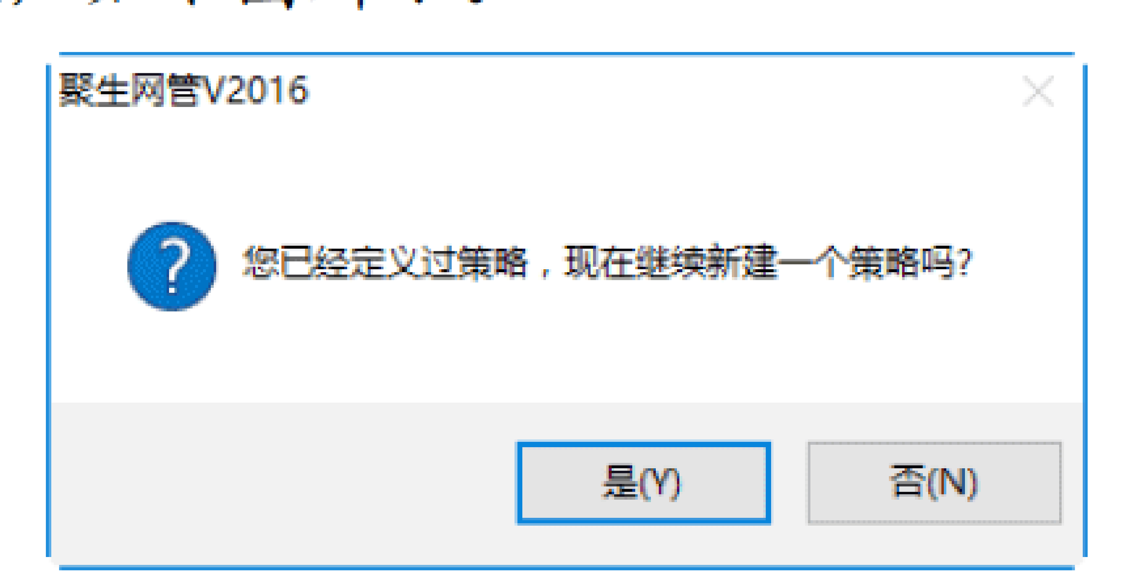
Step 06 单击“确定”按钮，将打开“编辑策略[局域网]的内容”对话框，在其中分别设置网络限制、带宽限制、P2P下载限制、流量限制、普通下载限制、游戏限制、股票限制、聊天限制、ACL规则、时间设置等选项卡，如下图所示。



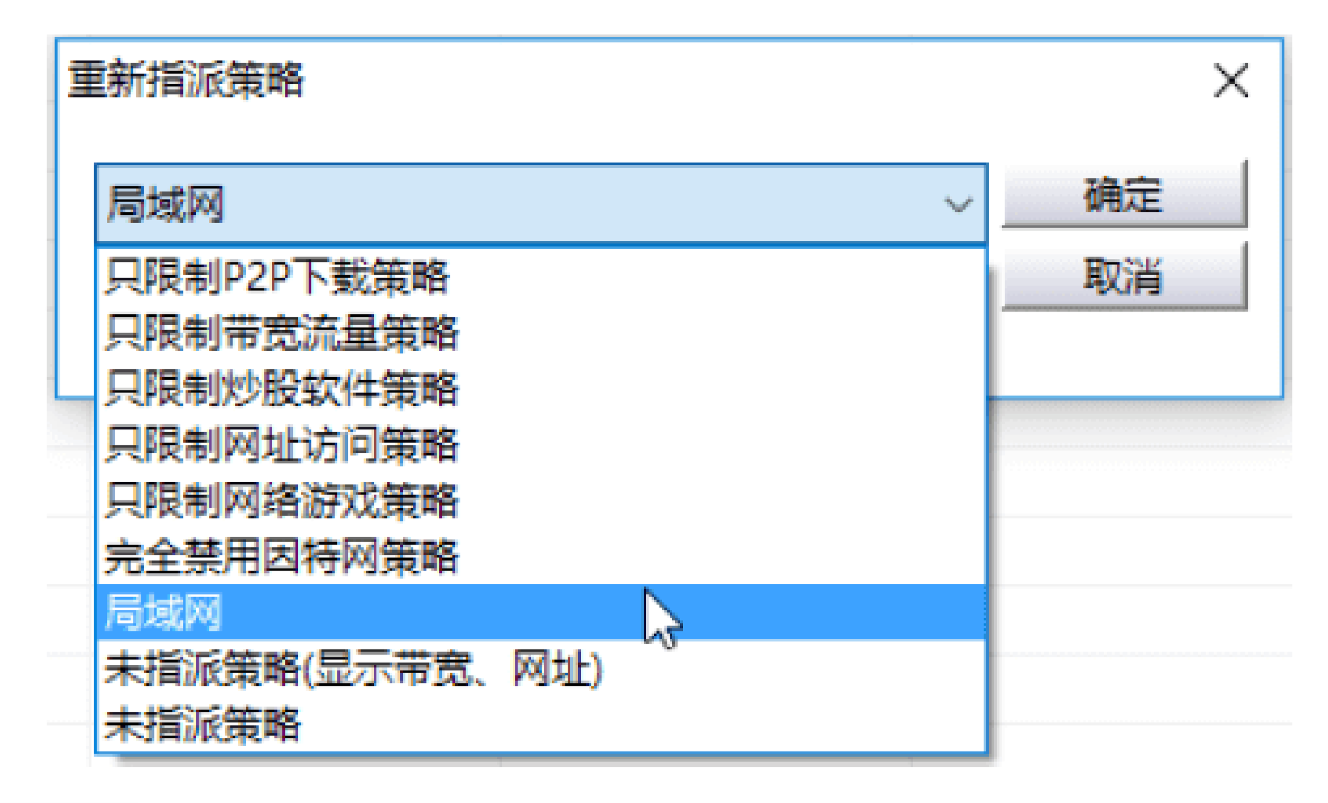
Step 07 设置完毕后，单击“确定”按钮，即可完成创建策略。单击“配置策略”按钮，打开“策略编辑”对话框，即可看到添加的策略，如下图所示。



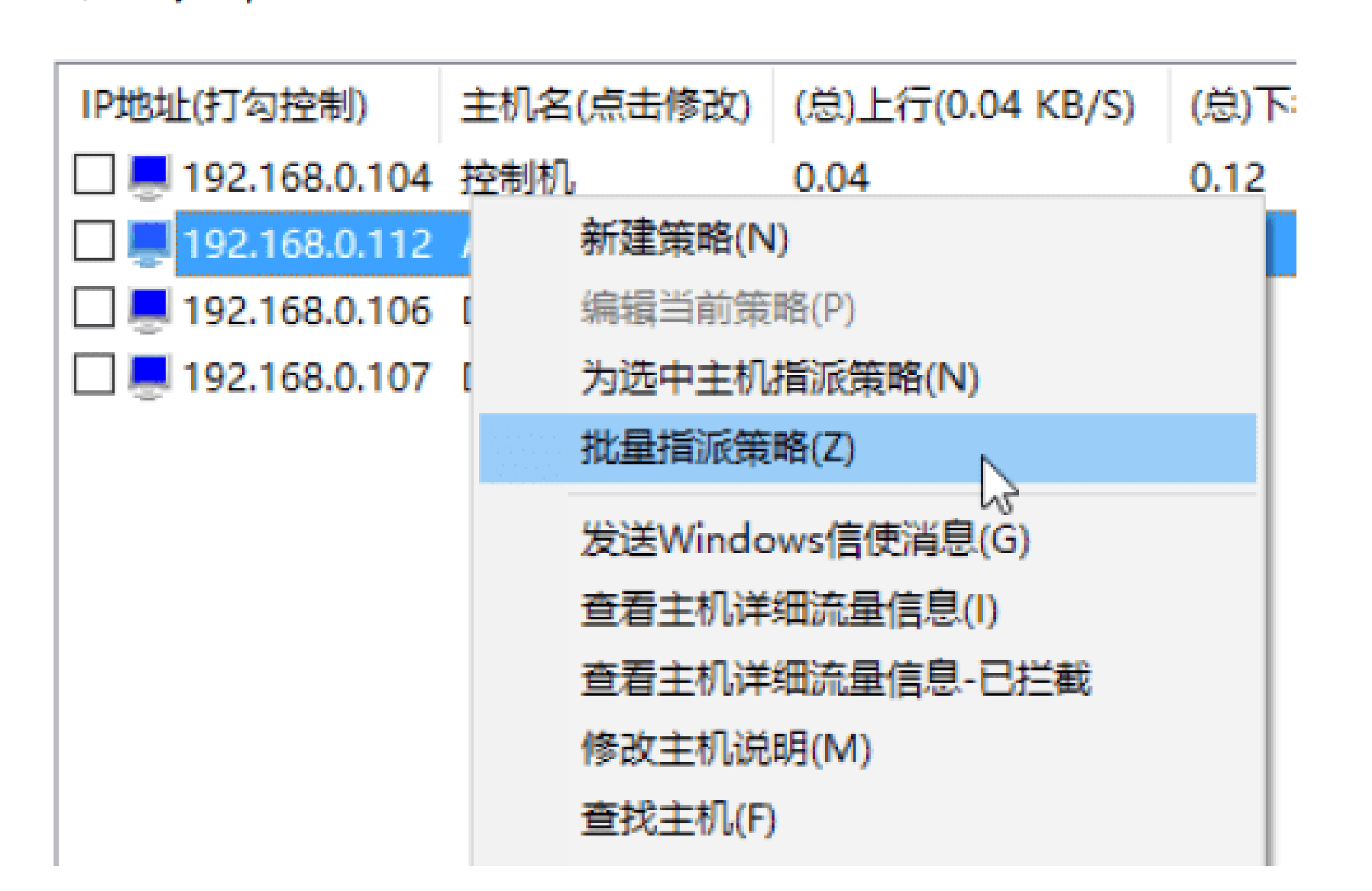
Step 08 建立好策略后，用户可以在主机列表窗格中，双击其他“未指派策略”的主机，为其指派已经建好的策略，也可以再建一个新的策略。若想再建一个策略，只需要双击该台主机，将弹出“您已经定义过策略，现在继续新建一个策略吗？”提示框，如下图所示。



Step 09 单击“是”按钮，可以继续新建一个策略；单击“否”按钮，将弹出“重新指派策略”对话框，如下图所示，可以重新指派刚才定义的策略，或者仍旧保持“未指派策略”状态，设置后单击“确定”按钮，即可成功设置指派策略。



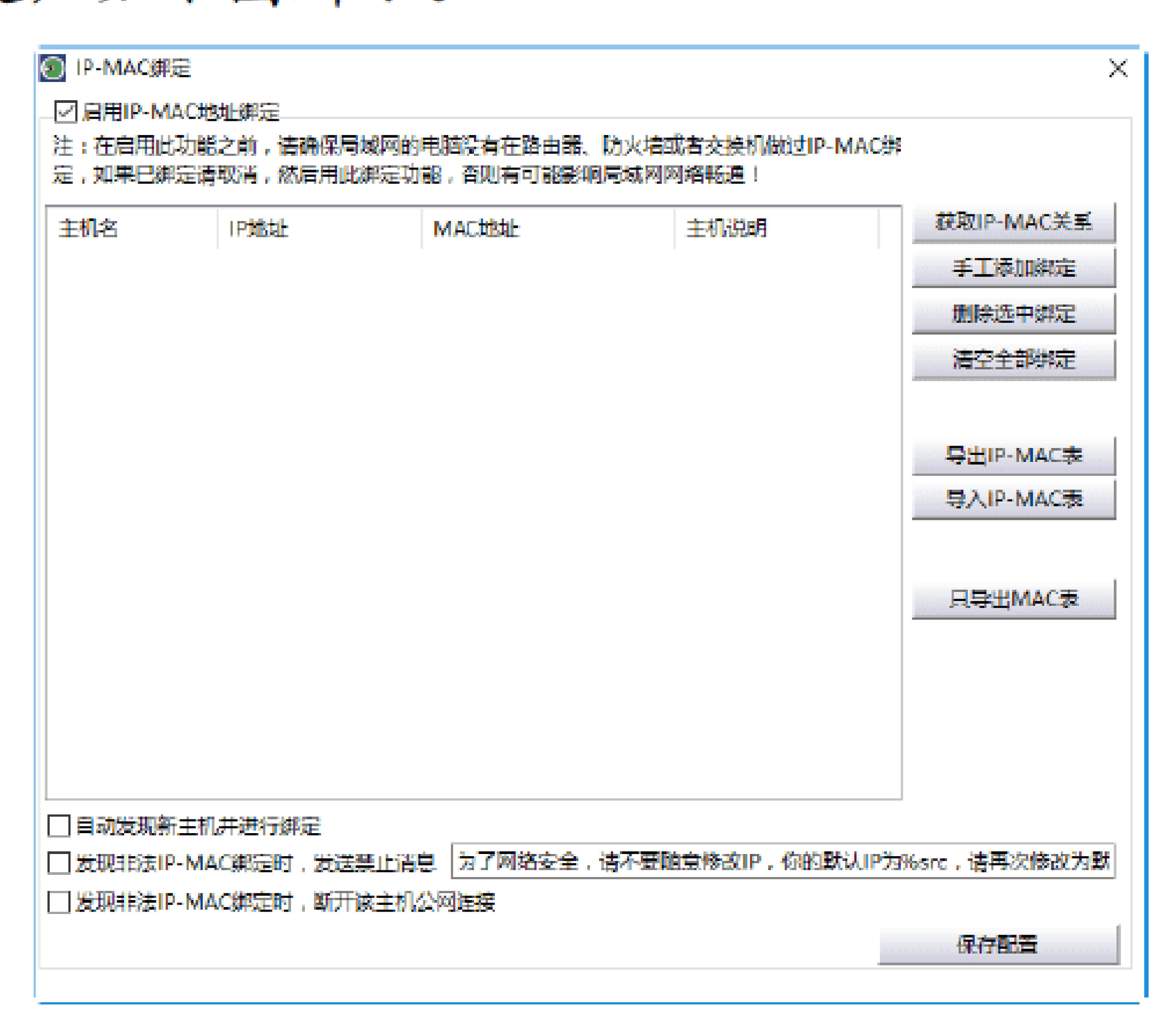
Step 10 如果想对所有的主机或者一部分主机都应用同一个策略，只需要在“聚生网管”主机列表窗格中右击鼠标，在弹出的快捷菜单中选择“批量指派策略”选项，如下图所示。



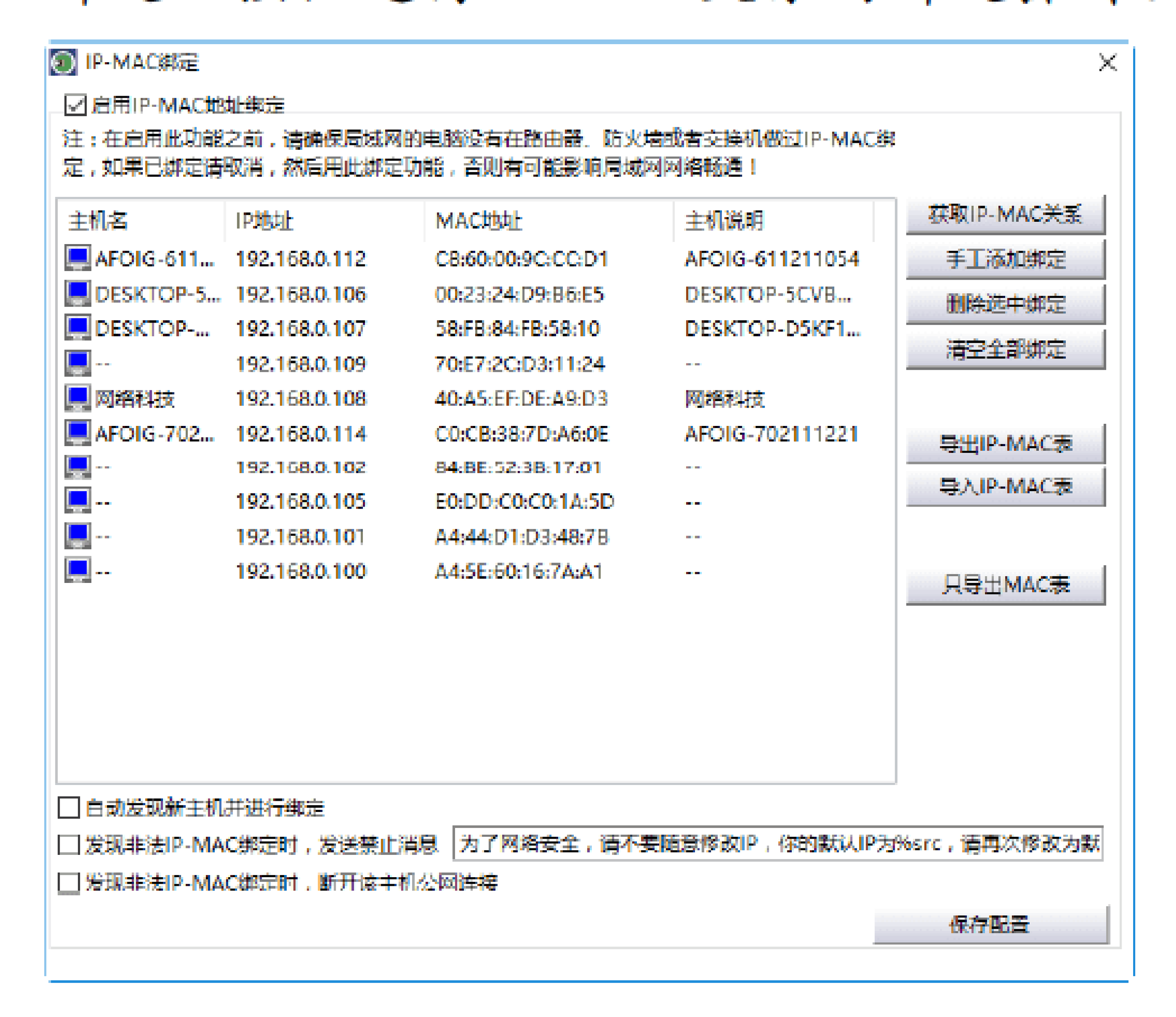
Step 11 打开“策略指派设置”对话框，如下图所示，左右两侧分别为已经指派策略的主机和未指派策略的主机，用户可以把其中的一个已经建立好策略的组或未建立策略的组里面的所有主机，全部指派到右侧的某个策略组里面或未指派的策略组里面；右侧的同样也可以指派到左侧的组里面。



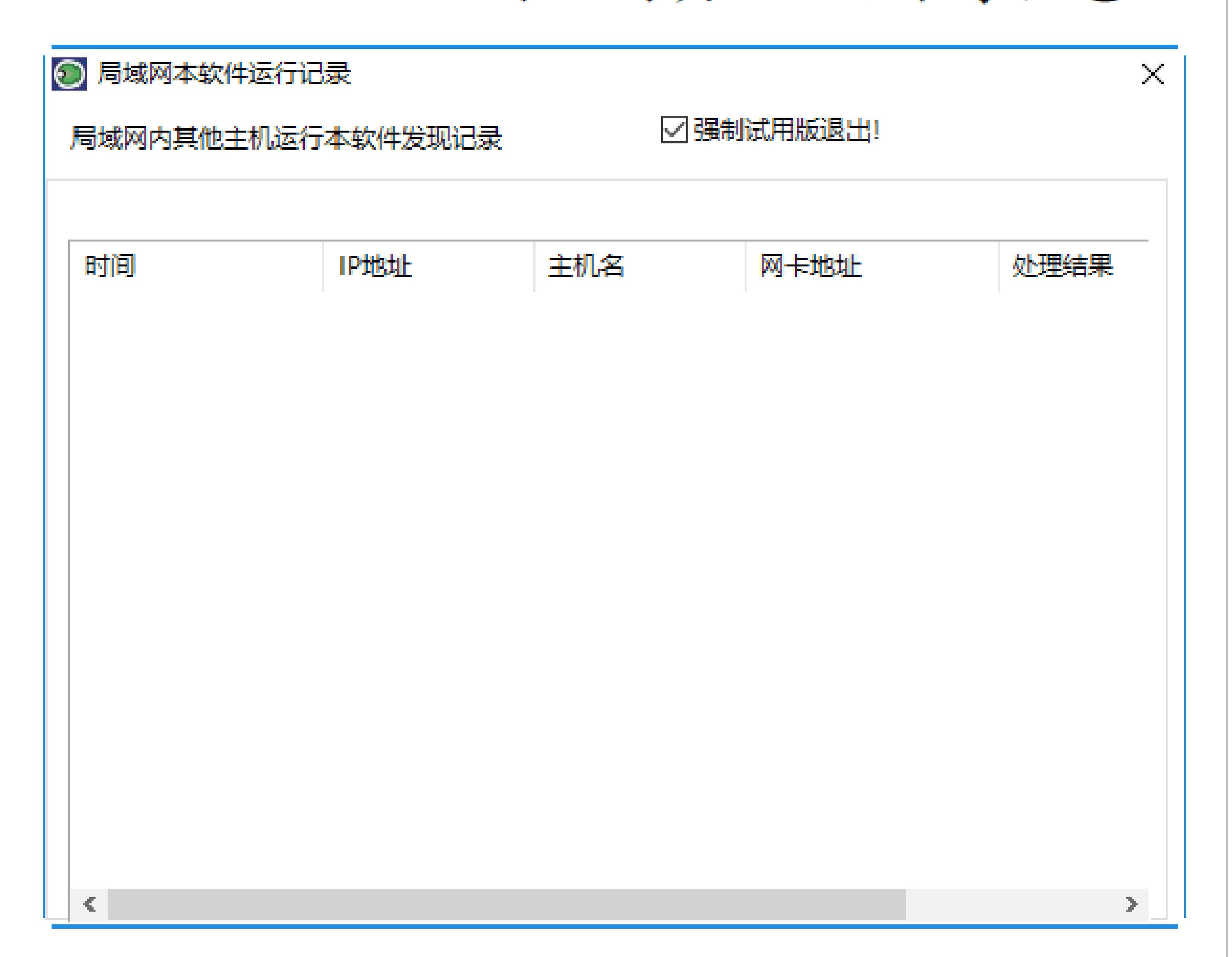
Step 12 在“聚生网管”主窗口中，单击“安全防御”按钮，在弹出的下拉列表中选择“IP-MAC绑定”选项，打开“IP-MAC绑定”对话框，在其中可以设置IP-MAC绑定，如下图所示。



Step 13 单击“获取IP-MAC关系”按钮，即可在左侧的窗格中显示获取的IP-MAC关系列表信息，如下图所示，然后通过单击“手工添加绑定”按钮进行IP-MAC关系的绑定操作。



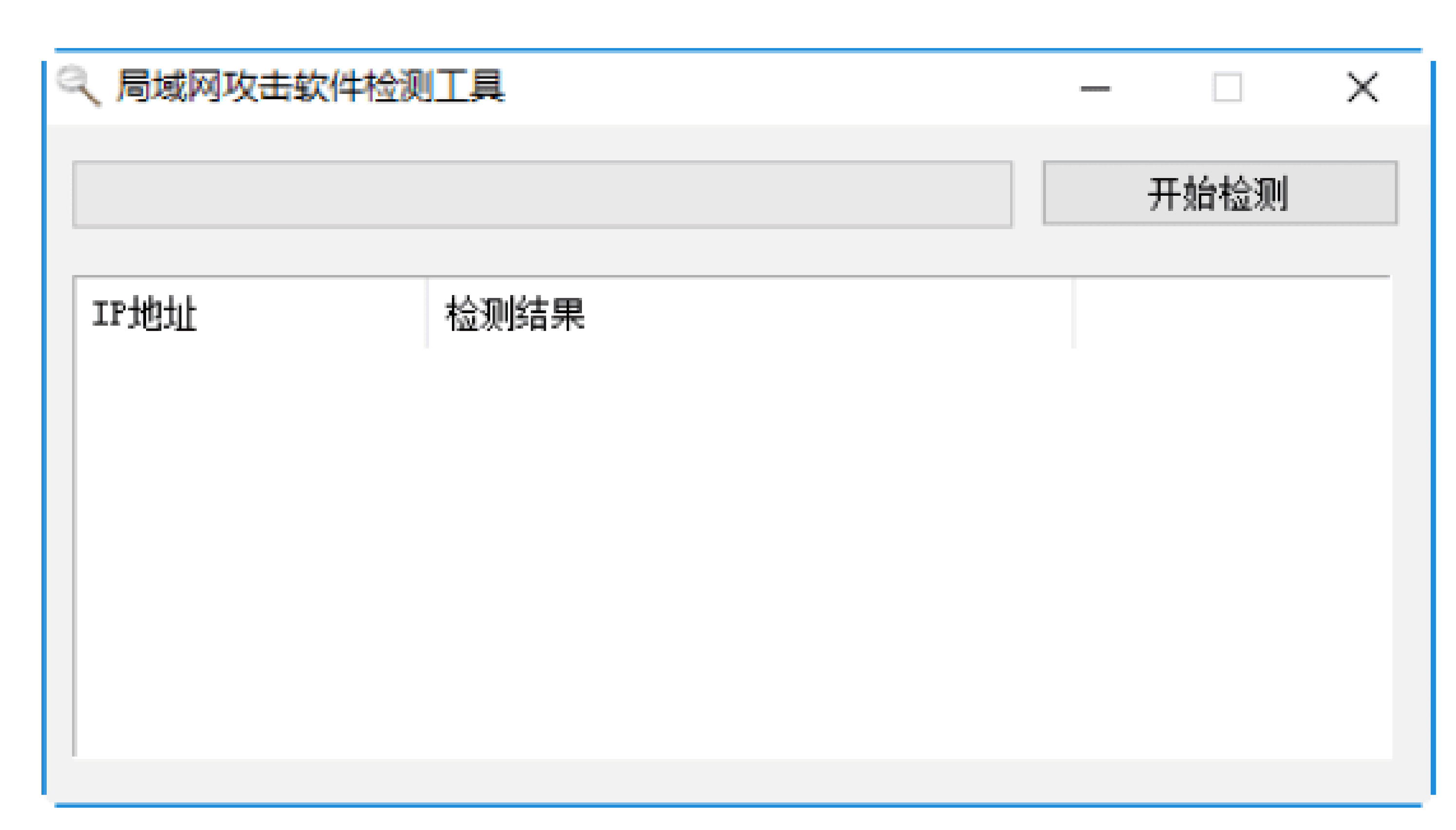
Step 14 为了保证局域网的安全，防止局域网内其他用户用“聚生网管”扰乱局域网，该工具还提供了防护“网内其他运行记录”功能。单击“安全防御”按钮，在弹出的下拉列表中选择“网内其他运行记录”选项，打开“局域网本软件运行记录”对话框，如下图所示，“聚生网管”的正式版可以强制测试版、试用版的聚生网管退出，并且记录下运行“聚生网管”主机名、运行时间、网卡地址、IP地址以及系统对其处理结果等信息。



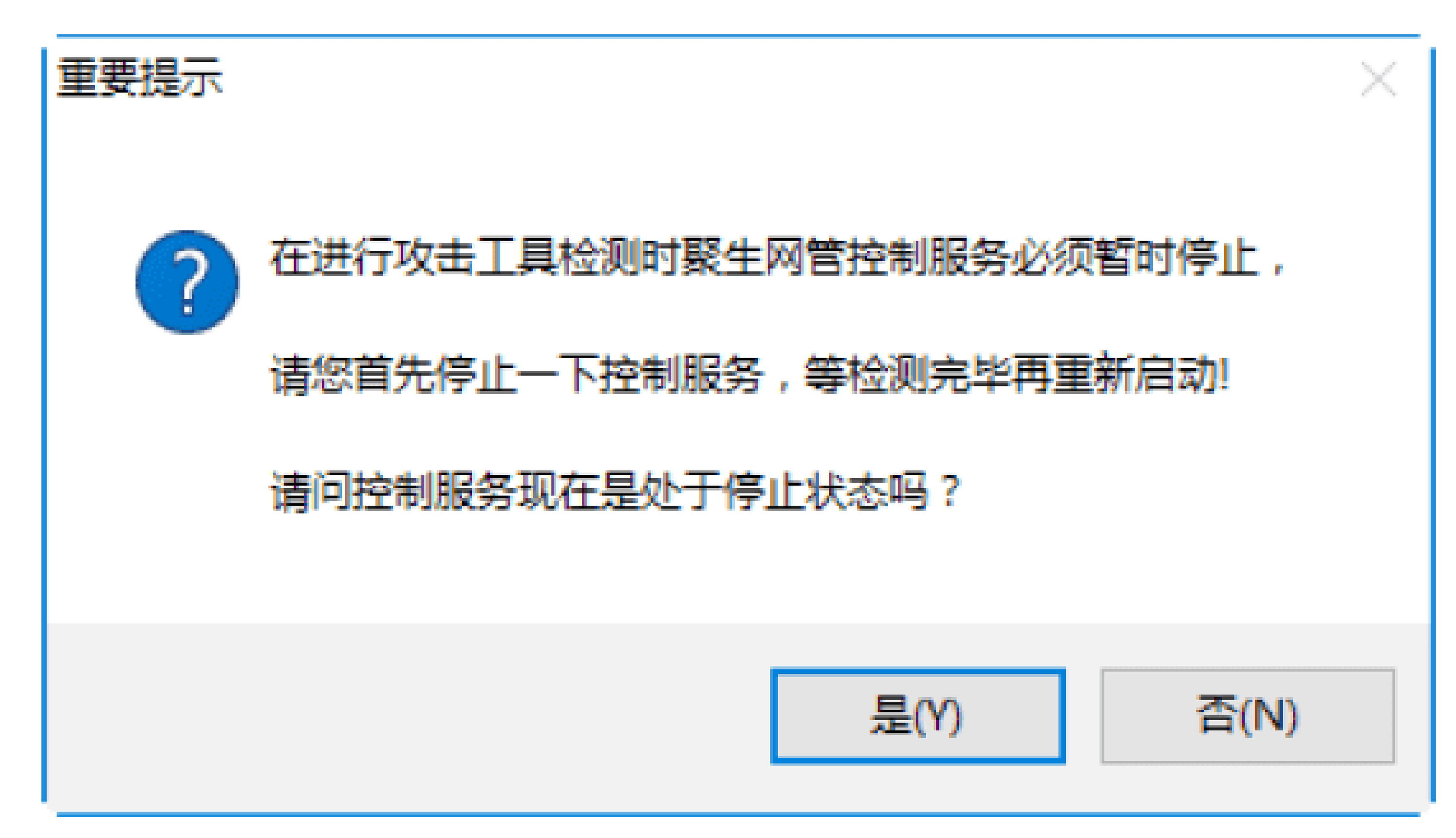
Step 15 利用“聚生网管”可以检测当前对局域网危害最为严重的三大工具：局域网终结者、网络剪刀手和网络执法官。在“聚生网管”主窗口中单击“安全防御”按钮，在弹出的下拉列表中选择“安全监测工具”选项，打开“安全监测工具”对话框，在其中即可看到局域网攻击检测工具和局域网ARP病毒、ARP攻击专项检测工具等，如下图所示。

安全监测工具
一、局域网混杂模式节点检测工具
本工具可以检测局域网内网卡处于混杂模式的节点，以发现嗅探软件或其他网管类软件
开始检测
二、局域网攻击检测工具
系统可以检测当前局域网三大工具软件：局域网终结者、网络剪刀手、网络执法官
开始检测
三、局域网ARP病毒、ARP攻击专项检测工具
(建议不超过10)
启用局域网ARP攻击防御功能
自动向局域网发送ARP攻击免疫信息
检测到ARP攻击时，自动加大免疫力度
0
检测到ARP攻击时记录危险主机
ARP攻击历史记录：
时间
IP地址
主机名
网卡地址
保存配置

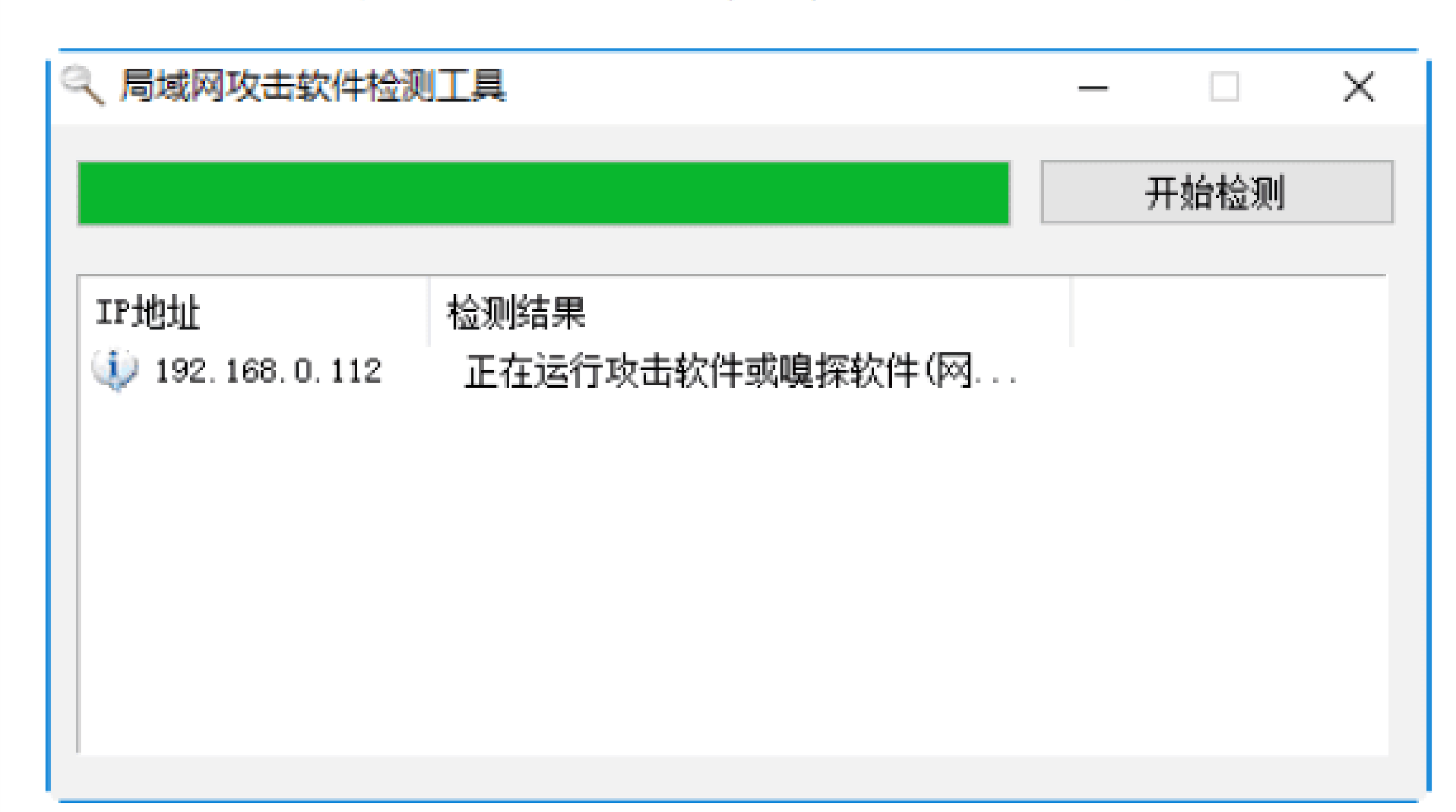
Step 16 单击“局域网攻击检测工具”栏目中的“开始检测”按钮，即可打开“局域网攻击软件检测工具”窗口，如下图所示。



Step 17 单击“开始检测”按钮，即可打开是否使控制服务处于停止状态提示框，如下图所示。



Step 18 单击“是”按钮，即可检测整个局域网中是否存在局域网攻击，同时将检测的结果显示在下面的列表中，如下图所示。



实战8：使用“长角牛网络监控机”保护局域网

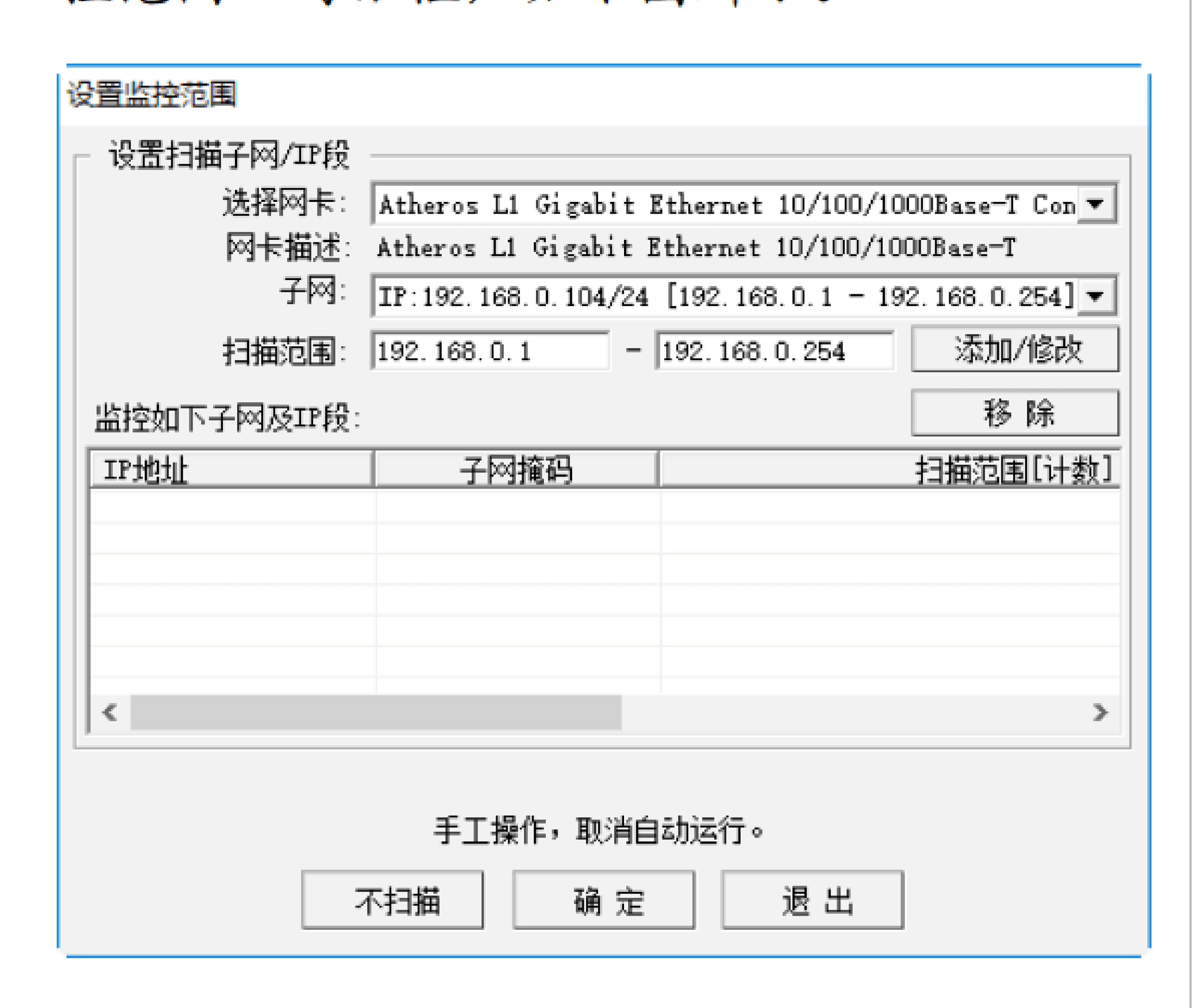


“长角牛网络监控机”只需在一台机器上运行，可穿透防火墙，实时监控、记录整个局域网用户的上线情况，可限制各用户上线时所用的IP、时段，并可将非法用户踢出局域网。

1. 查看主机信息

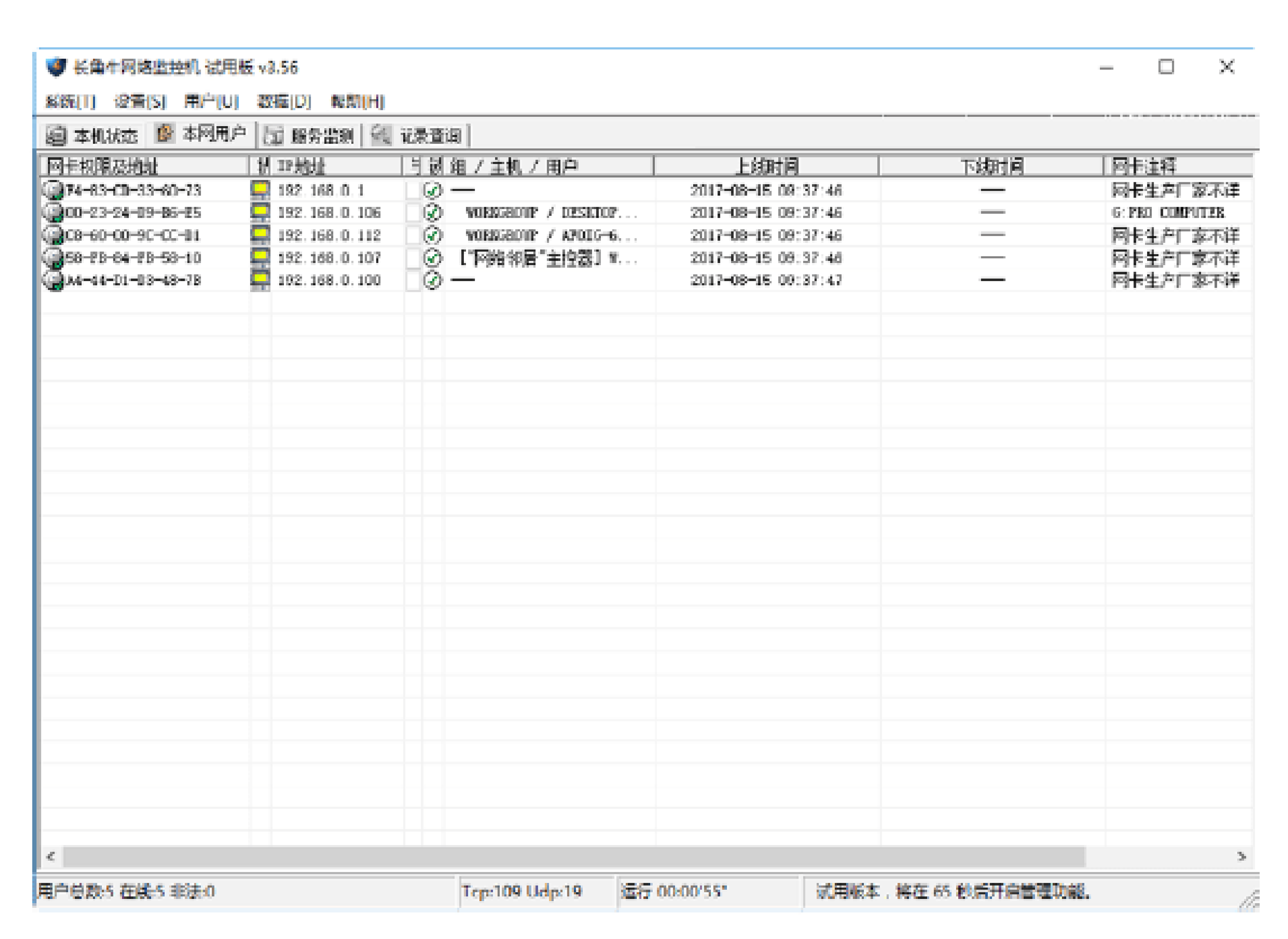
利用该工具可以查看局域网中各个主机的信息，如用户属性、在线纪录、记录查询等。具体操作步骤如下。

Step 01 在下载并安装“长角牛网络监控机”工具，选择“开始”→“所有应用”→Netrobocop选项，即可打开“设置监控范围”对话框，如下图所示。

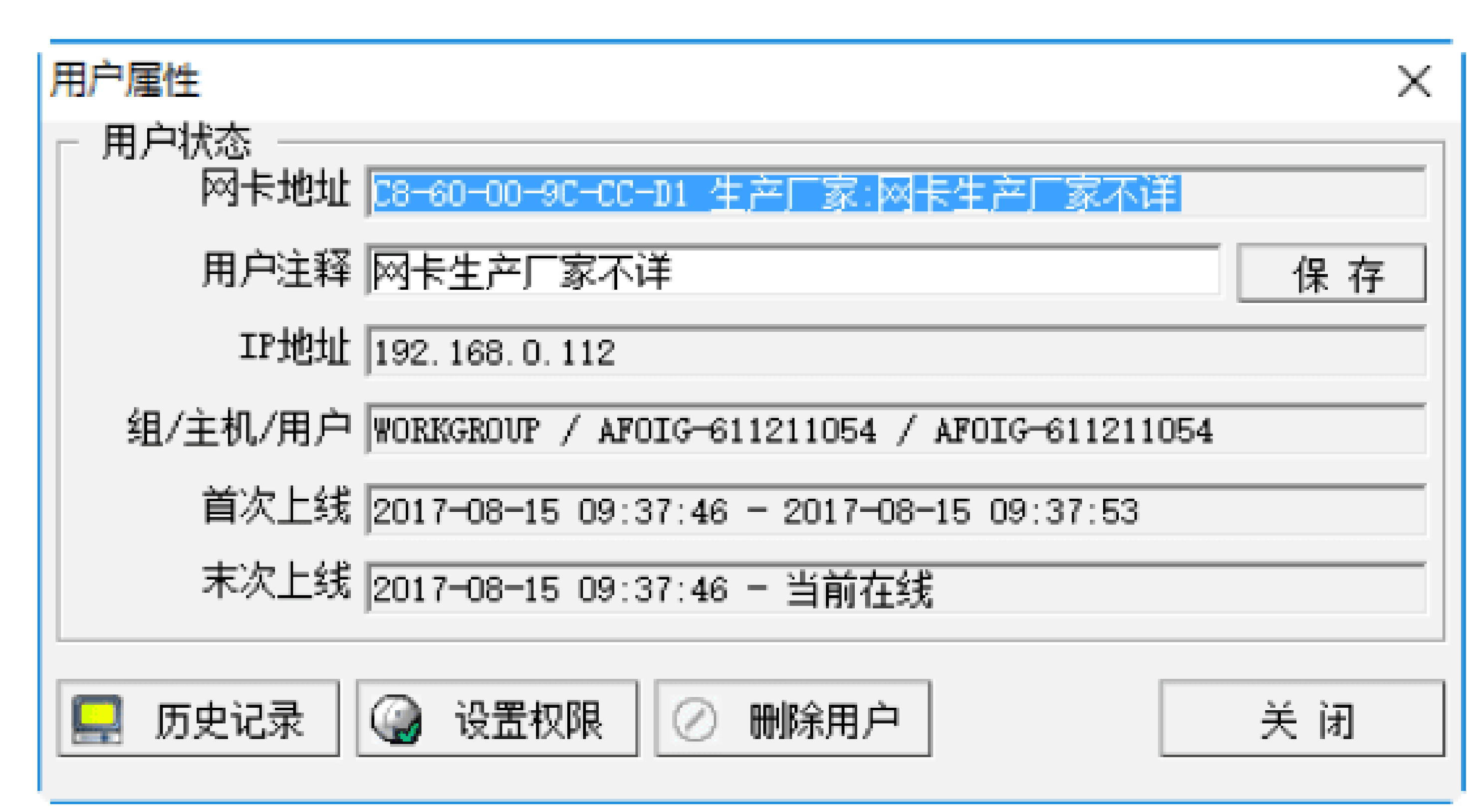


Step 02 在设置好网卡、子网、扫描范围等属性之后，单击“添加/修改”按钮，即可将设置的扫描范围添加到“监控如下子网及IP段”列表中，如下图所示。

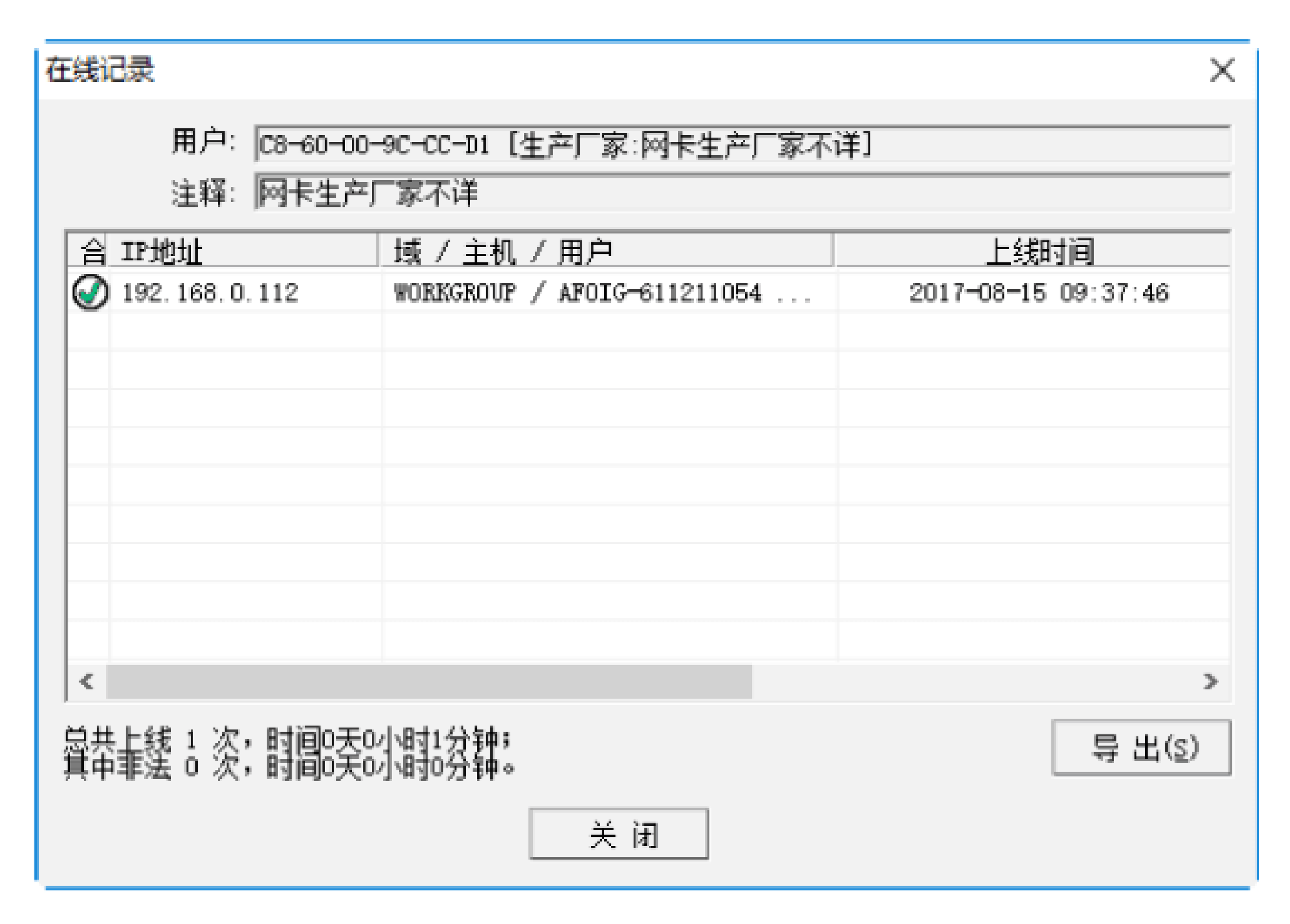
Step 03 选中刚添加的IP段，单击“确定”按钮，即可打开“长角牛网络监控机”主窗口，在其中即可看到设置IP地址段内的主机的各种信息，如网卡权限地址、IP地址、上线时间等，如下图所示。



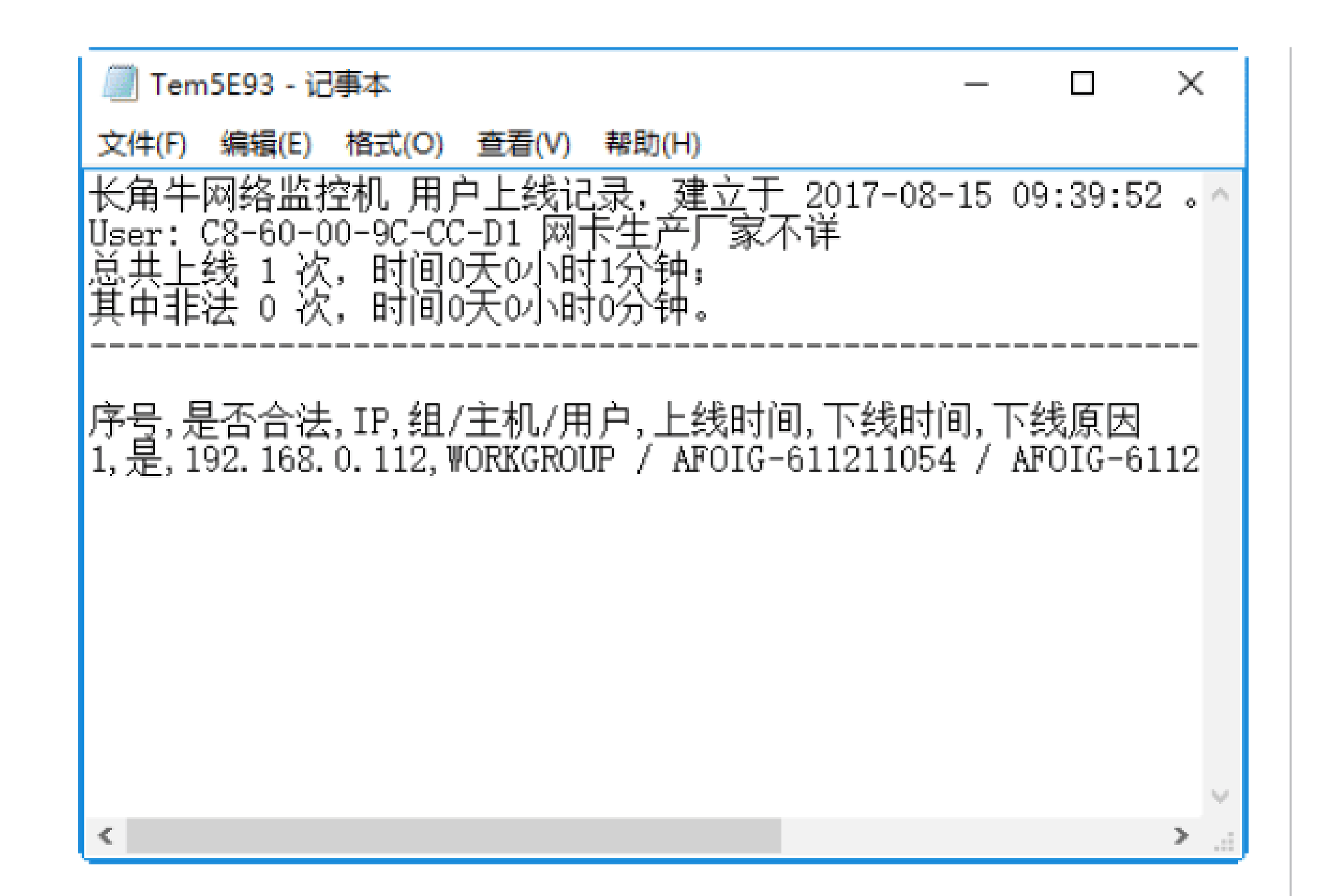
Step 04 在“长角牛网络监控机”窗口的计算机列表中双击需要查看的对象，即可打开“用户属性”对话框，如下图所示。



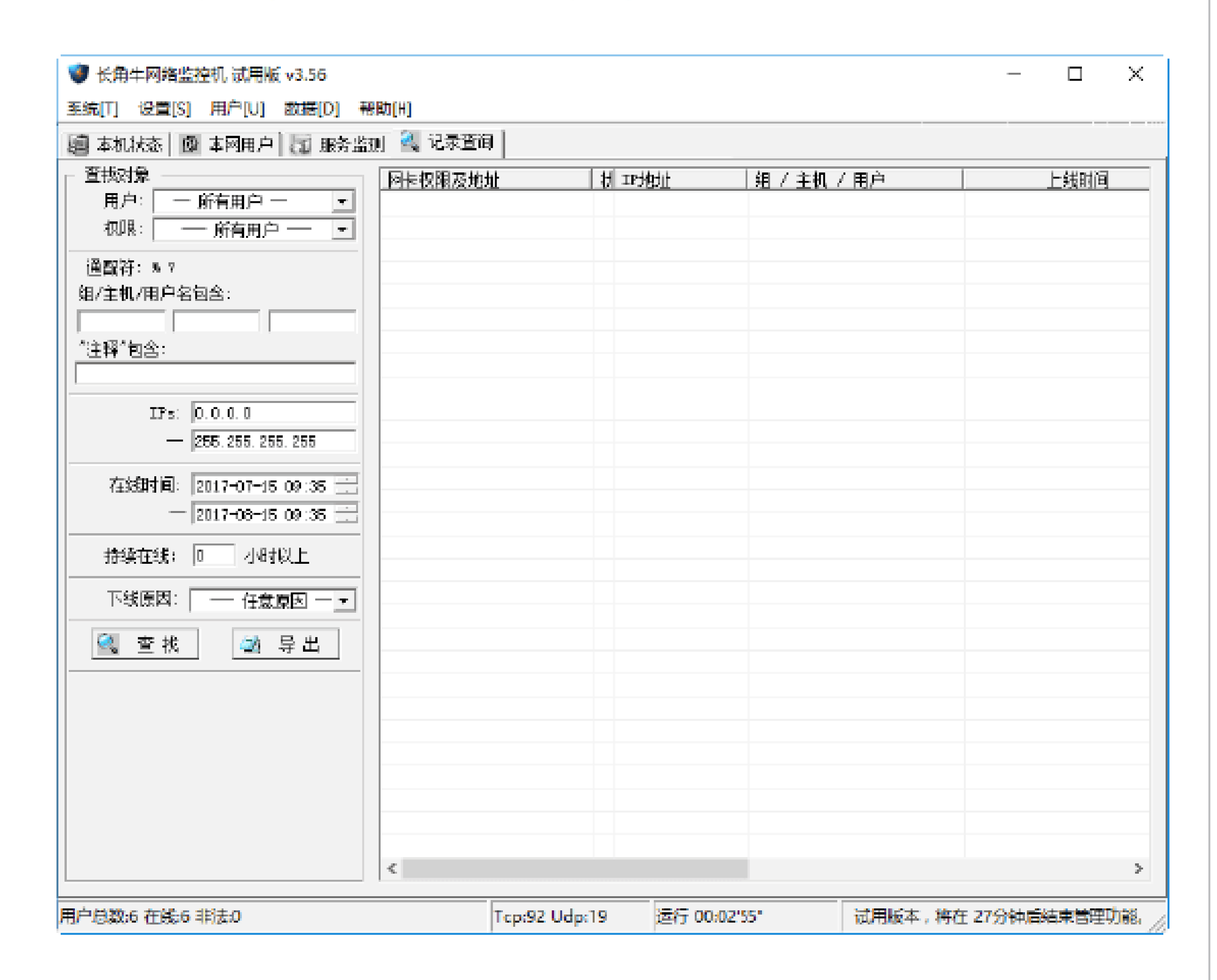
Step 05 单击“历史记录”按钮，即可打开“在线记录”对话框，在其中查看该计算机的上线情况，如下图所示。



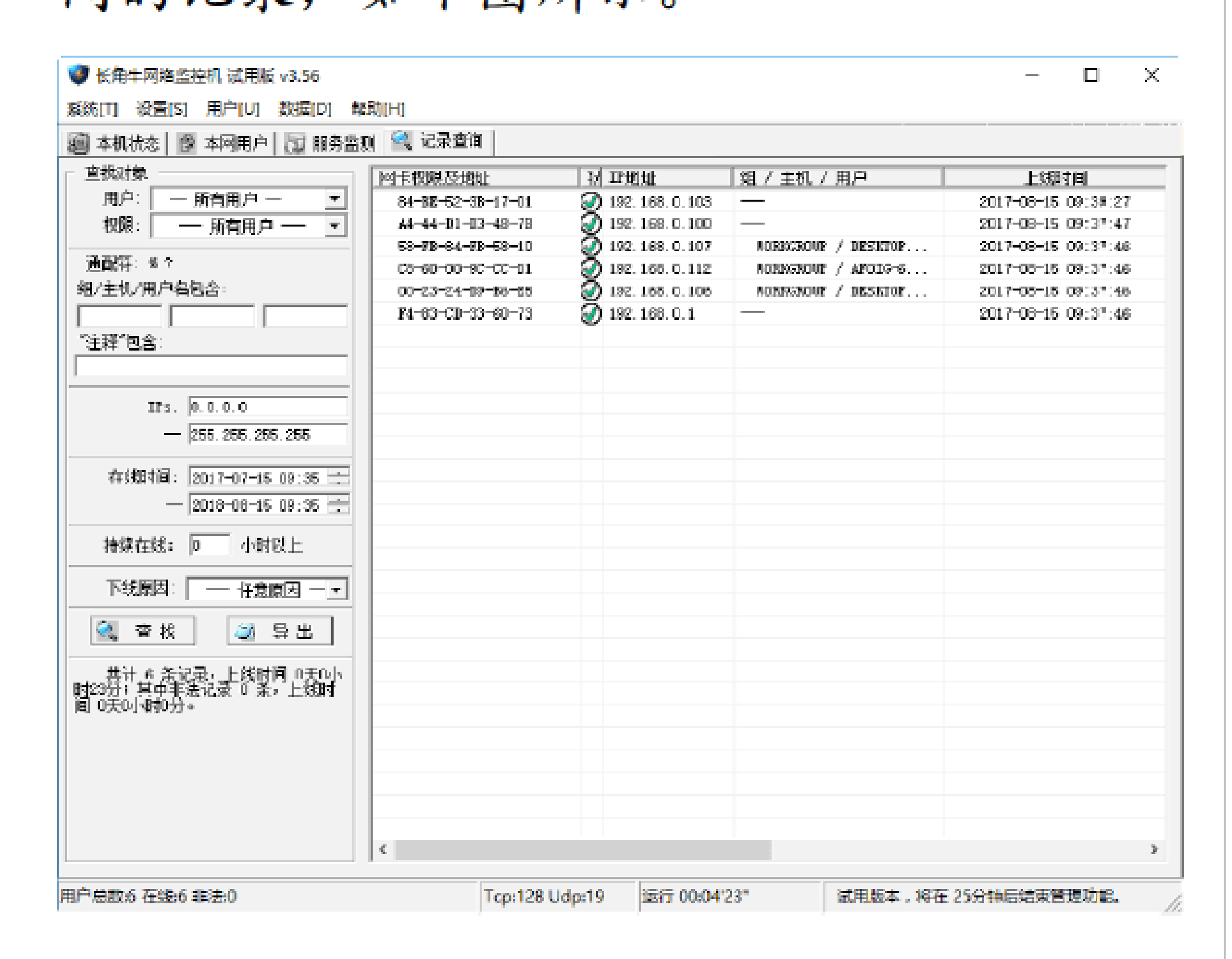
Step 06 单击“导出”按钮，即可将该计算机的上线记录保存为文本文件，如下图所示。



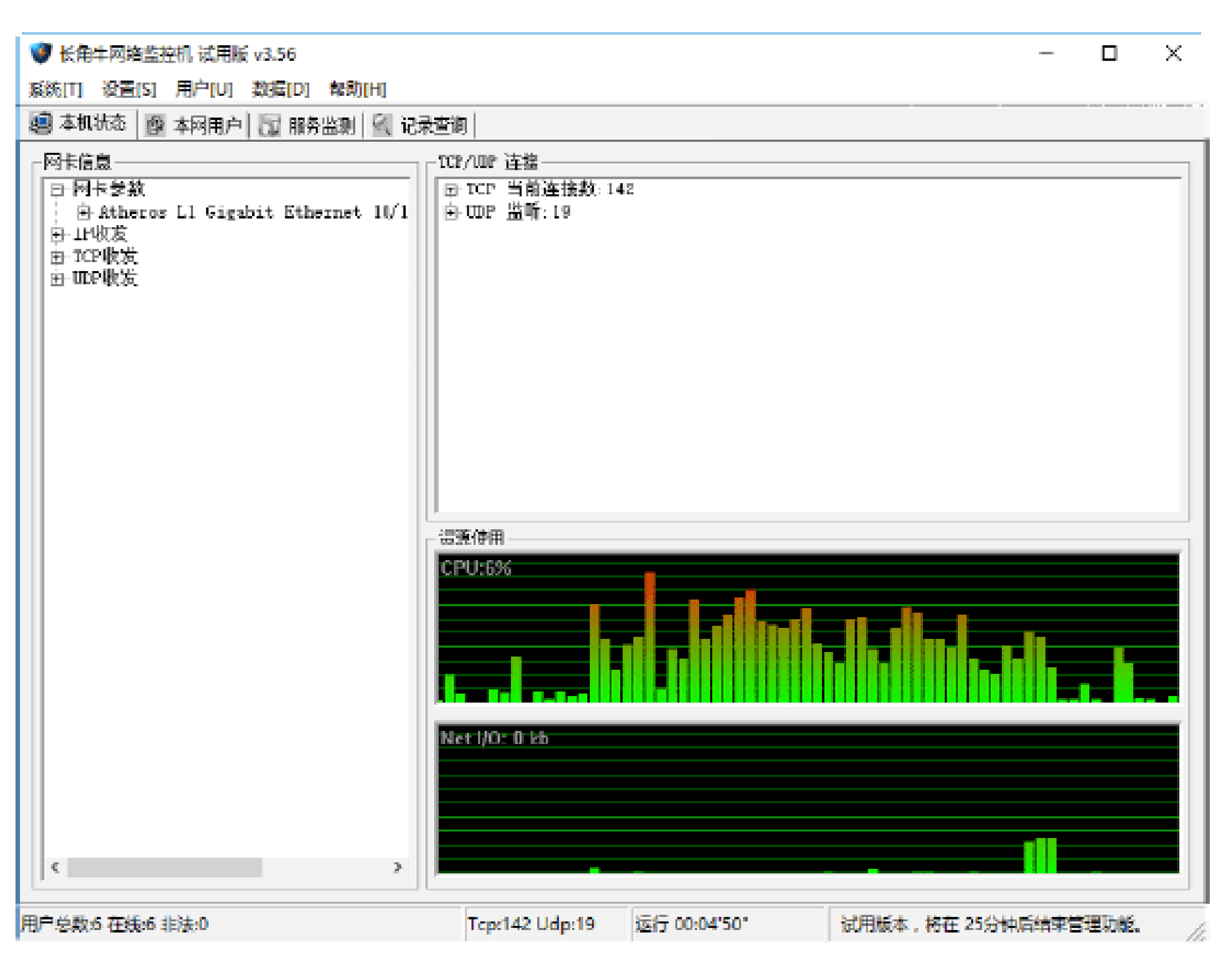
Step 07 在“长角牛网络监控机”窗口中单击“记录查询”按钮，即可打开“记录查询”子窗口，如下图所示。



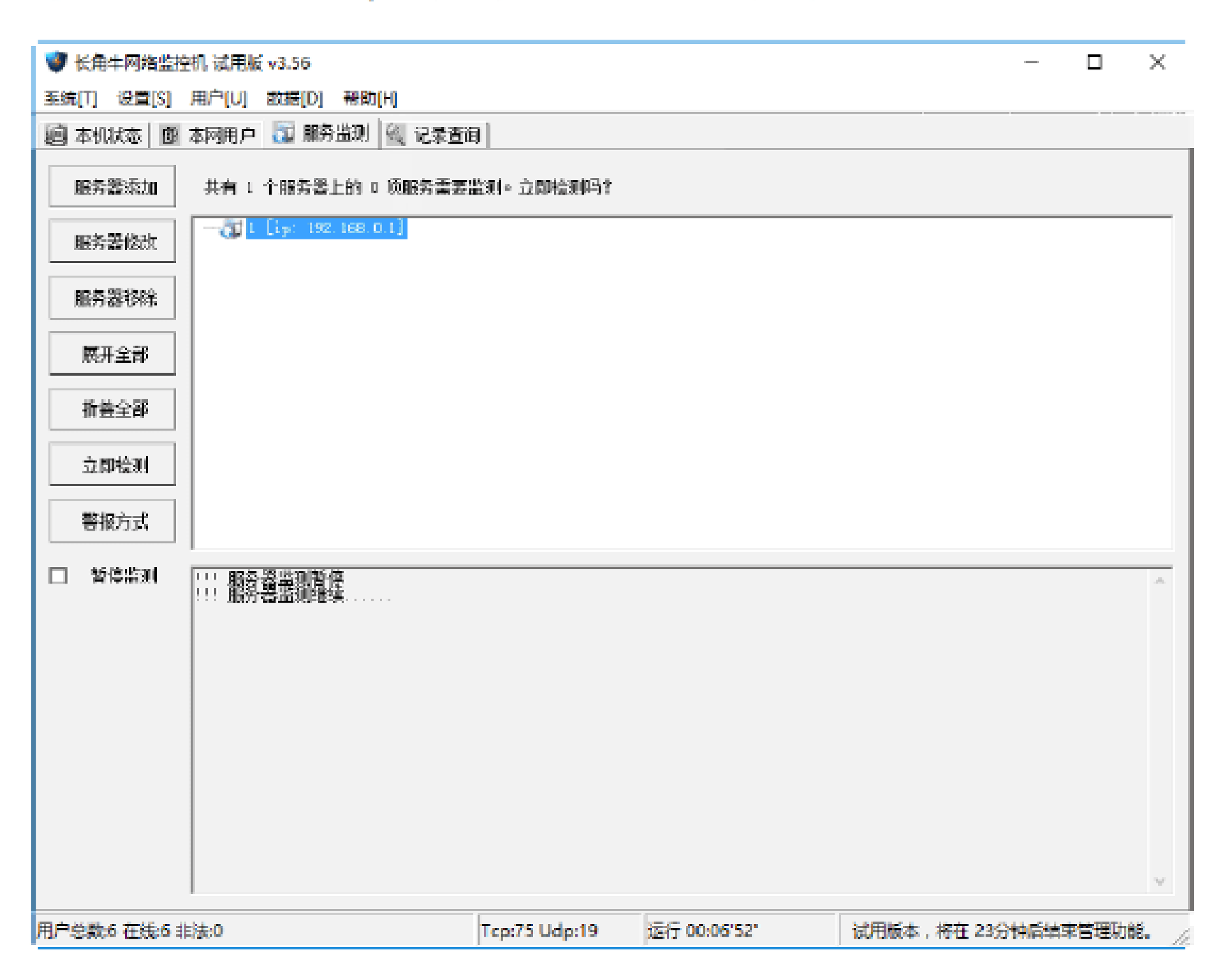
Step 08 在“用户”下拉列表中选择要查询用户对应的网卡地址；在“在线时间”文本框中设置该用户的在线时间，然后单击“查找”按钮，即可找到该主机在指定时间的记录，如下图所示。



Step 09 在“长角牛网络监控机”窗口中单击“本机状态”按钮，即可打开“网卡信息”子窗口，在其中即可看到本机的网卡参数、IP收发、TCP收发、UDP收发等信息，如下图所示。



Step 10 在“长角牛网络监控机”窗口中单击“服务监测”按钮，可进行服务器添加、修改、移除等操作，如下图所示。



2. 设置局域网

除收集局域网内各计算机的信息之外，“长角牛网络监控机”工具还可以对局域网中的各计算机进行网络管理，可以在局域网内的任一台计算机上安装该软件，实现对整个局域网内的计算机进行管理。具体的操作步骤如下。

Step 01 在“长角牛网络监控机”窗口中选择“设置”→“关键主机组”选项，即可打开“关键主机组设置”对话框，如下图所示，在“选择关键主机组”下拉框中选择

相应的主机组，并在“组名称”文本框中输入相应的名称，再在“组内IP”列表框中输入相应的IP组。最后单击“全部保存”按钮，即可完成关键主机组的设置操作。

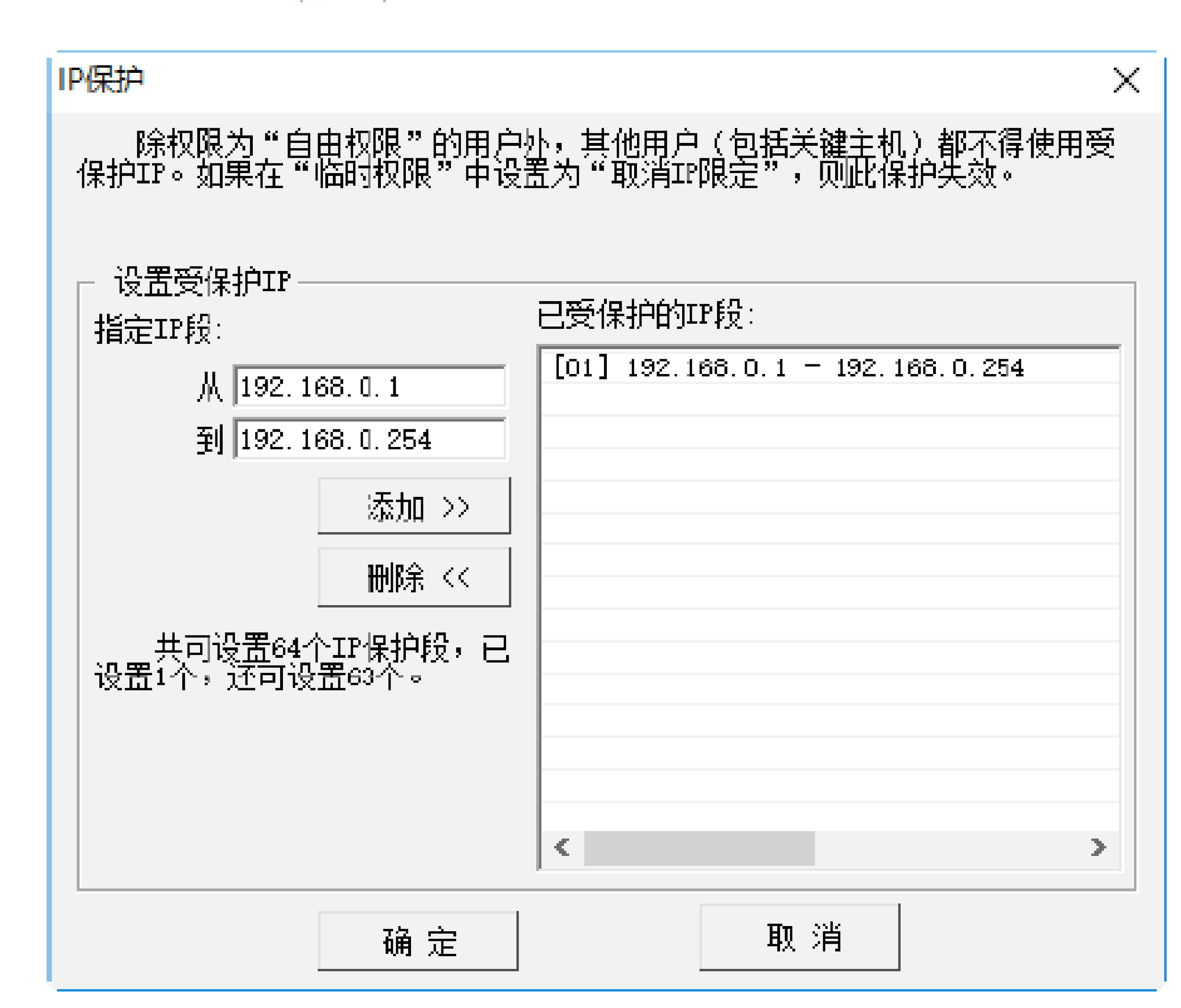


提示：“关键主机组”是由管理员指定的IP地址，可以是网关、其他计算机或服务器等。管理员将指定的IP存入“关键主机组”后，即可令非法用户仅断开与“关键主机组”的连接而不断开与其他计算机的连接。

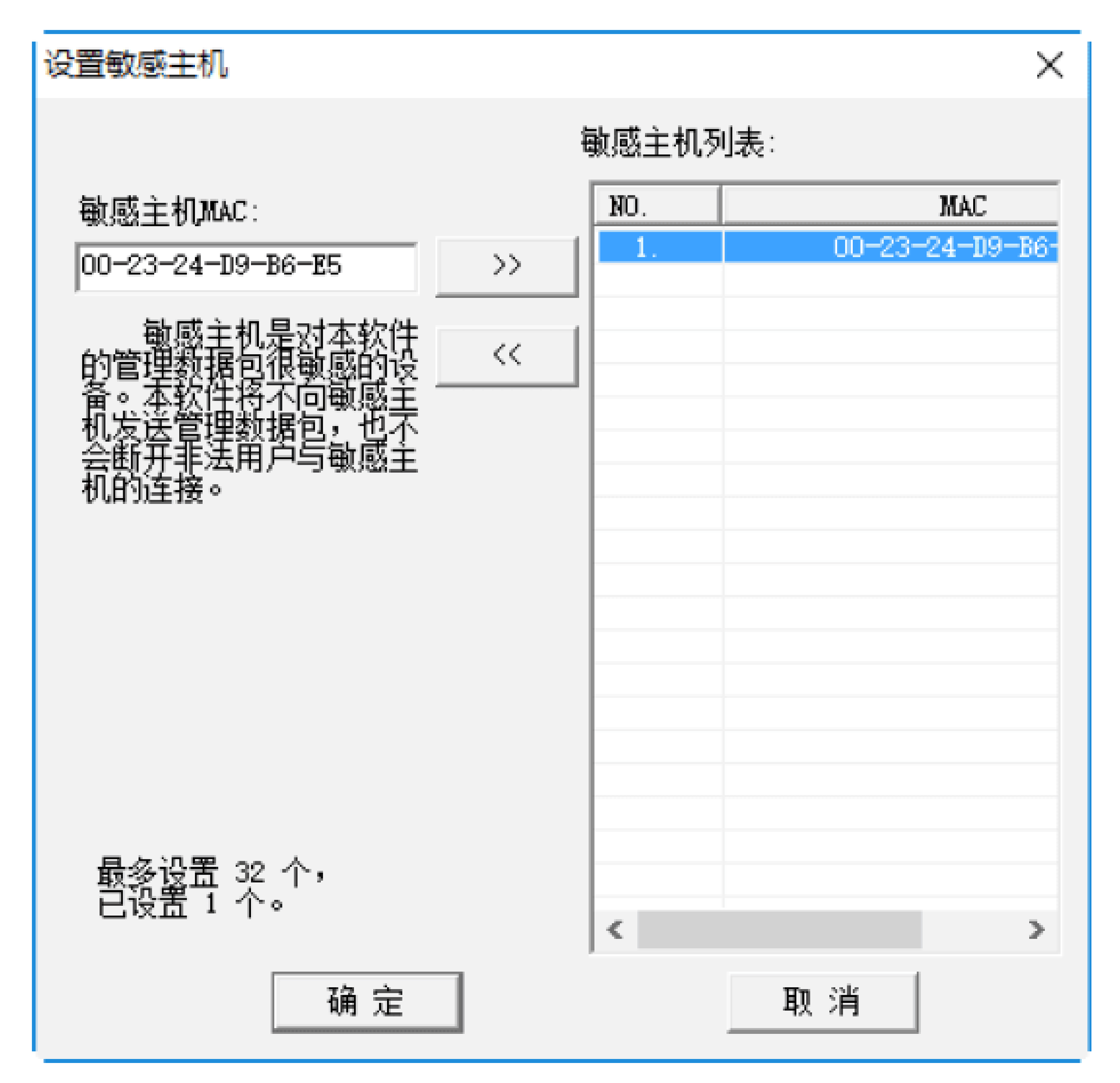
Step 02 在“长角牛网络监控机”窗口中选择“设置”→“默认权限”选项，即可打开“用户权限设置”对话框，如下图所示，选中“受限用户，若违反以下权限将被管理”单选按钮，设置“IP限制”“时间限制”和“组/主机/用户名限制”等选项。这样当目标计算机与局域网连接时，“长角牛网络监控机”将按照设定的选项对该计算机进行管理。



Step 03 可以利用“长角牛网络监控机”工具保护指定的IP地址段。在“长角牛网络监控机”窗口中选择“设置”→“IP保护”选项，即可打开“IP保护”对话框，如下图所示。在其中设置要保护的IP段后，单击“添加”按钮，即可将该IP段添加到“已受保护的IP段”列表中。

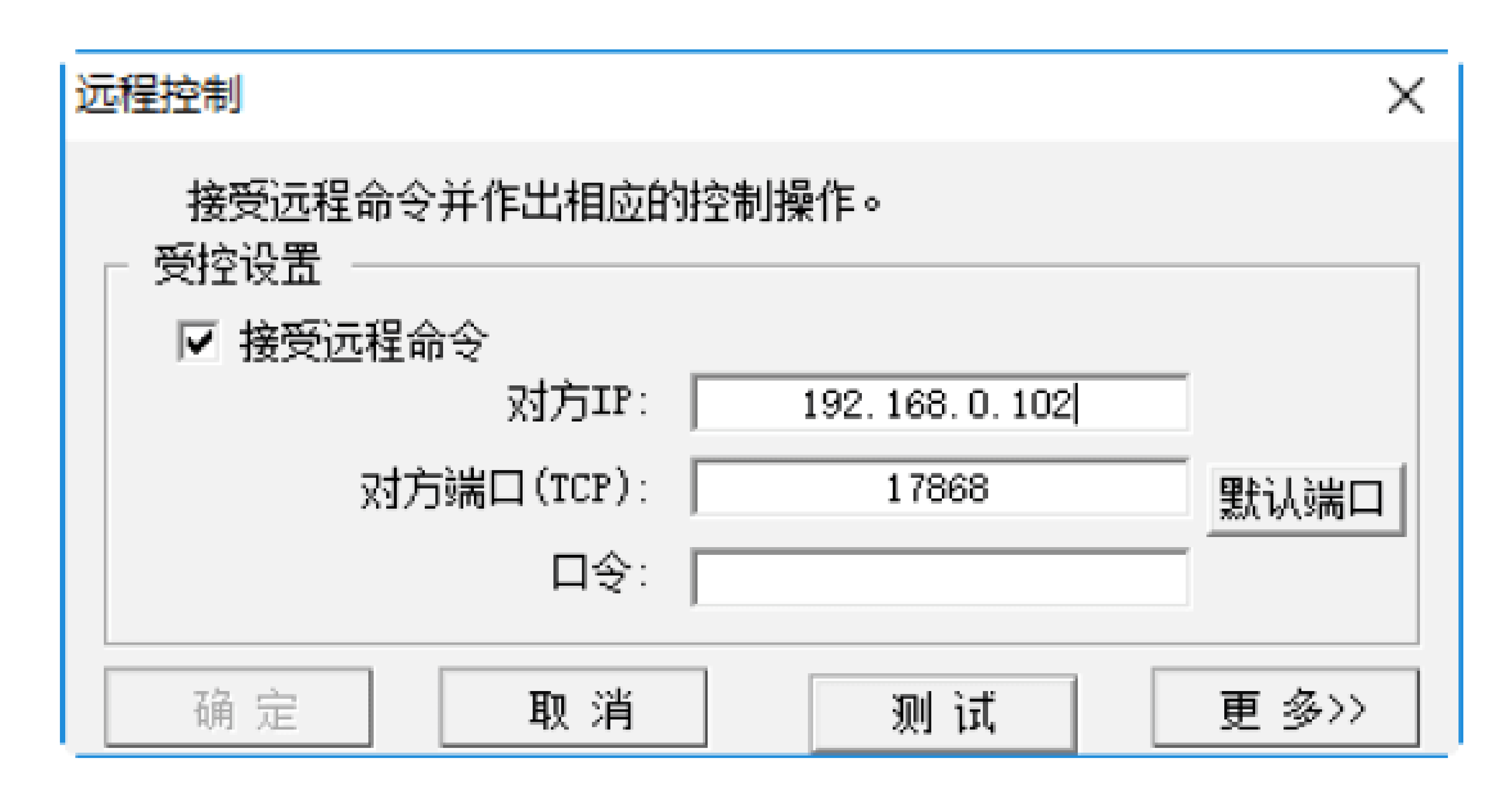


Step 04 在“长角牛网络监控机”工具中还可以敏感主机。在“长角牛网络监控机”窗口中选择“设置”→“敏感主机”选项，即可打开“设置敏感主机”对话框，如下图所示，在“敏感主机MAC”文本框中输入目标主机的MAC地址后单击 >> 按钮，即可将该主机设置为敏感主机。



Step 05 在“长角牛网络监控机”窗口中选择“设置”→“远程控制”选项，即可打开“远程控制”对话框，如下图所示，在其中勾选“接受远程命令”复选框，并输入

目标主机的IP地址和口令后，即可对该主机进行远程控制。



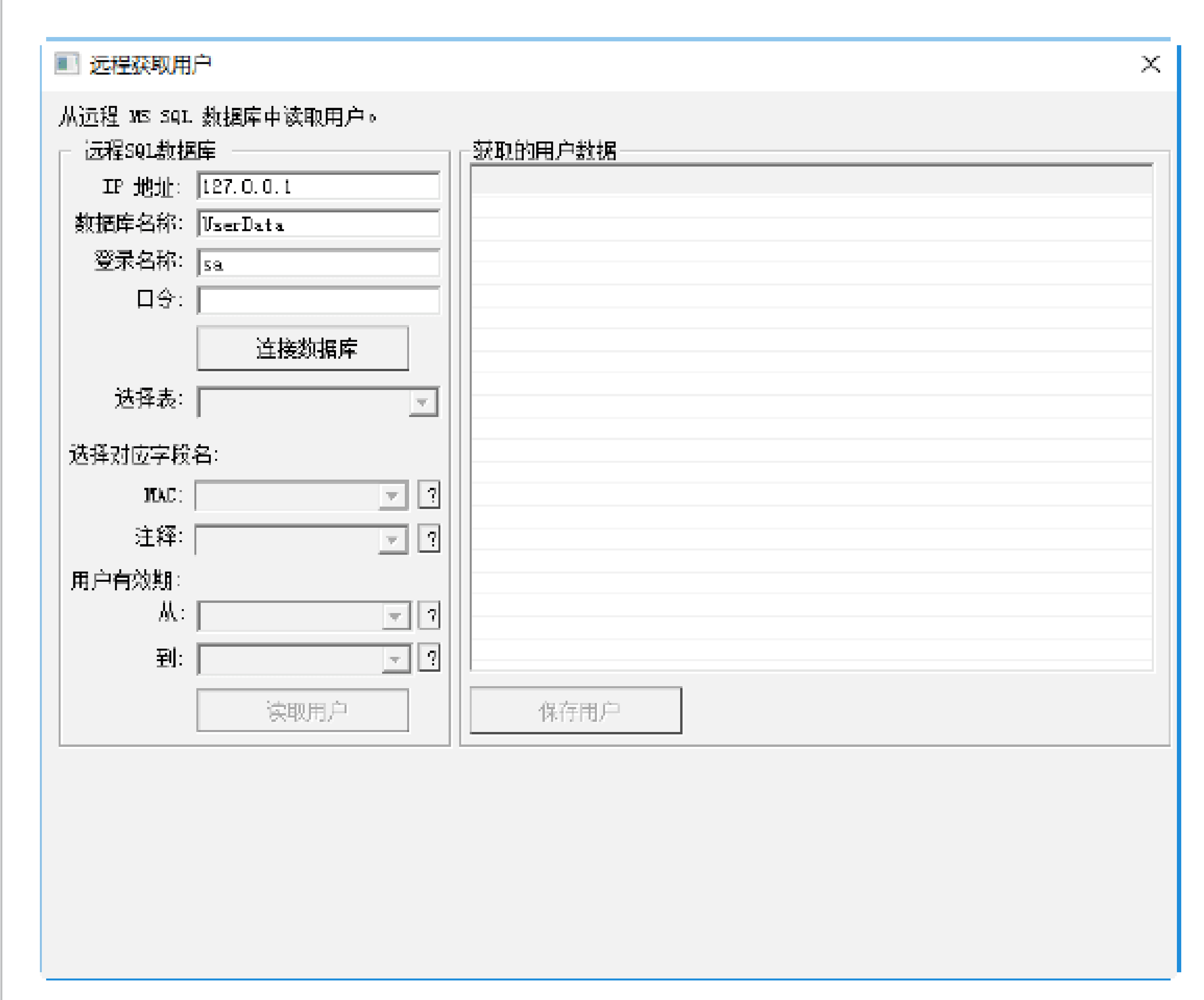
Step 06 在“长角牛网络监控机”窗口中选择“设置”→“主机保护”选项，即可打开“主机保护”对话框，如下图所示，勾选“启用主机保护”复选框，输入要保护主机的IP地址和网卡地址，单击“加入”按钮，即可将该主机添加到“受保护主机”列表中。

主机保护
启用主机保护　保护强度：8
设置
IP地址：192.168.0.106
加入>>
移出<<
网卡地址：Mac 00-23-24-D9-B6-E5
受保护主机
no.　ip地址　网卡
1　192.168.0.106　00-23-24-
保护全网(虚拟机中慎用)
保护自身
以如下方式自动封锁ARP欺骗：
IP 冲突　断开与所有主机连
帮助
停用主机保护并且启动时不再显示
确 定

Step 07 在“长角牛网络监控机”工具中还可以添加新的用户。在“长角牛网络监控机”窗口中选择“用户”→“添加用户”选项，即可打开“New user（新用户）”对话框，如下图所示，在MAC文本框中输入新用户的MAC地址，单击“保存”按钮，即可实现添加新用户操作。

New user
添加新用户
MAC：00-10-24-56-89-Df
注释：手工加入，2017-08-15 09:50。
权限设置　保 存　取 消

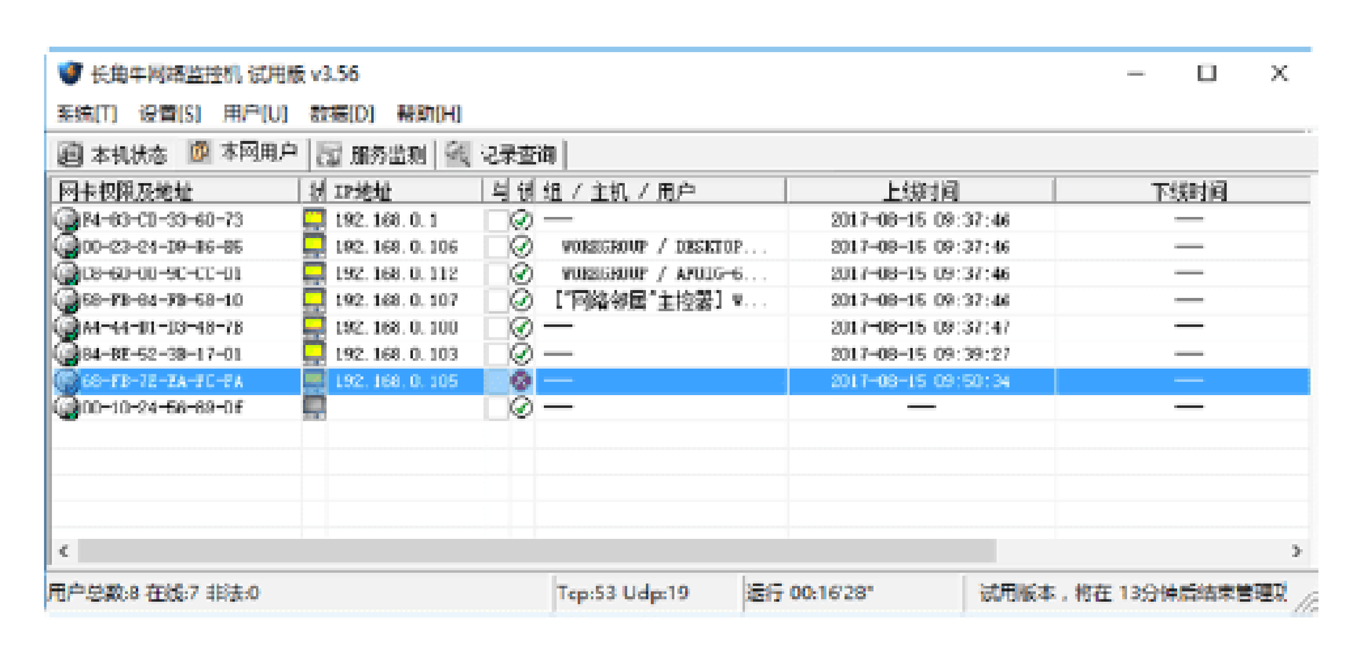
Step 08 在“长角牛网络监控机”窗口中选择“用户”→“远程添加”选项，即可打开“远程获取用户”对话框，如下图所示，在其中输入远程计算机的IP地址、数据库名称、登录名称以及口令之后，单击“连接数据库”按钮，即可从该远程主机中读取用户。



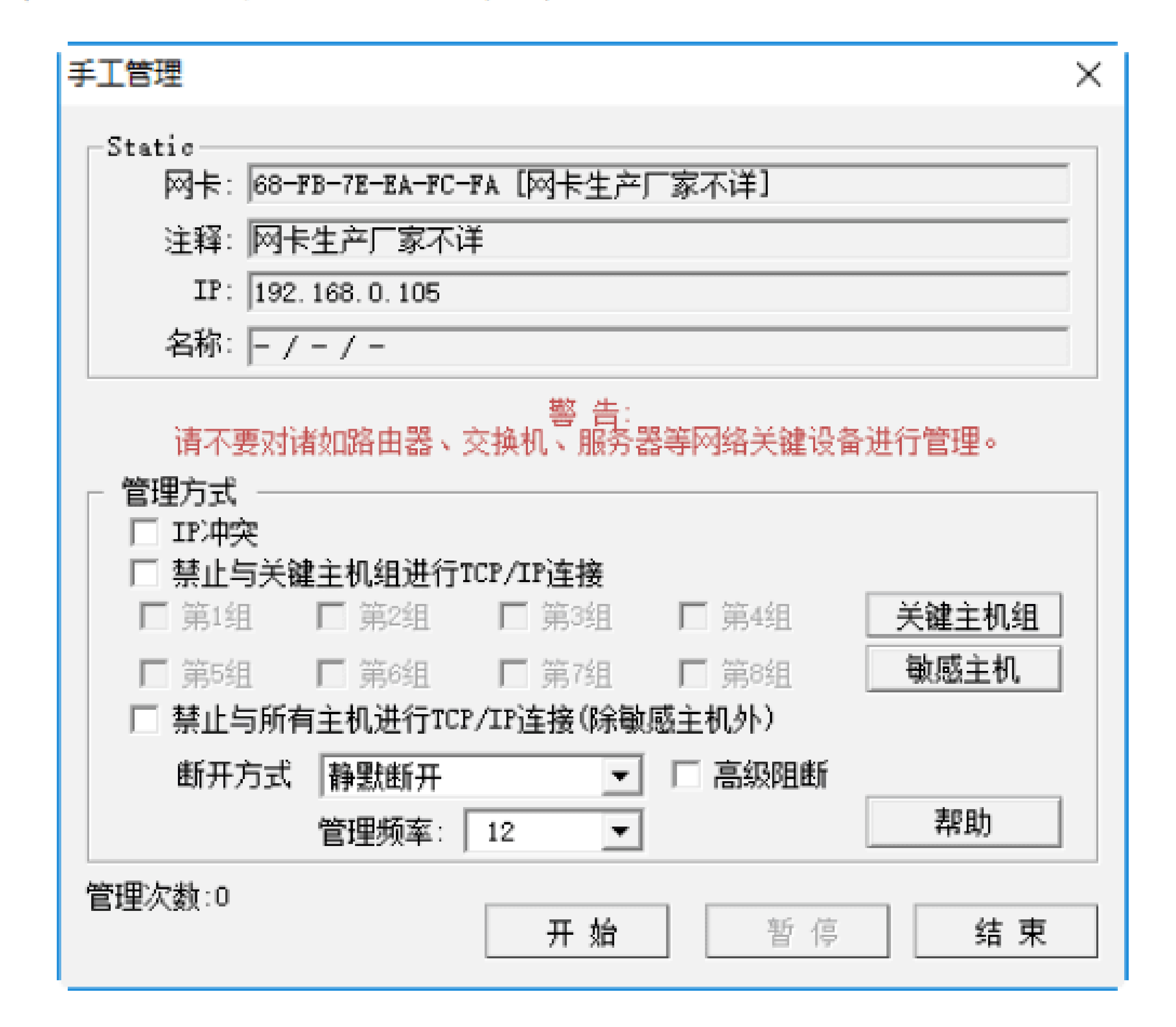
Step 09 如果禁止局域网内某一台计算机的网络访问权限，则可在“长角牛网络监控机”窗口内右击该计算机，在弹出的快捷菜单中选择“锁定/解锁”选项，即可打开“锁定/解锁”对话框，如下图所示。

锁定/解锁
网卡：68-FB-7E-EA-FC-FA [网卡生产厂家不详]
注释：网卡生产厂家不详
警 告：
请不要对诸如路由器、交换机、服务器等网络关键设备进行锁定。
锁定方式：
不锁定（解锁）
禁止与以下关键主机组的TCP/IP连接
第1组　第2组　第3组　第4组　设置
第5组　第6组　第7组　第8组
禁止与所有主机的TCP/IP连接(除敏感主机外)
确 定　取 消

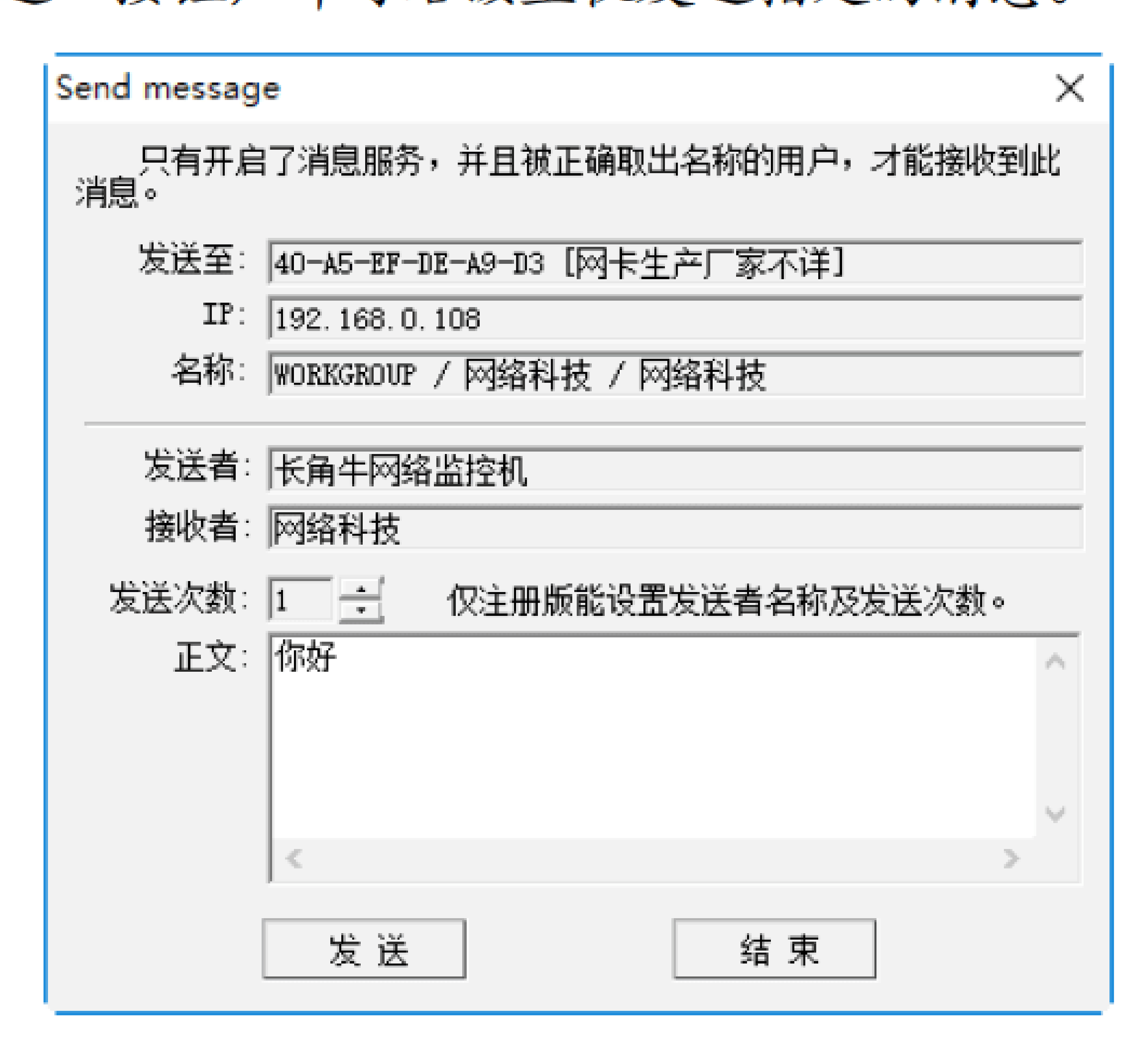
Step 10 在其中选择目标计算机与其他计算机（或关键主机组）的连接方式之后，单击“确定”按钮，即可禁止该计算机访问相应的连接，如下图所示。



Step 11 在“长角牛网络监控机”窗口右击某台计算机，在弹出的快捷菜单中选择“手工管理”选项，即可打开“手工管理”对话框，在其中即可手动设置对该计算机的管理方式，如下图所示。



Step 12 在“长角牛网络监控机”工具中还可以给指定的主机发送消息。在“长角牛网络监控机”窗口右击某台计算机，在弹出的快捷菜单中选择“发送消息”选项，即可打开“Send message（发送消息）”对话框，如下图所示，在其中输入要发送的消息后，单击“发送”按钮，即可给该主机发送指定的消息。



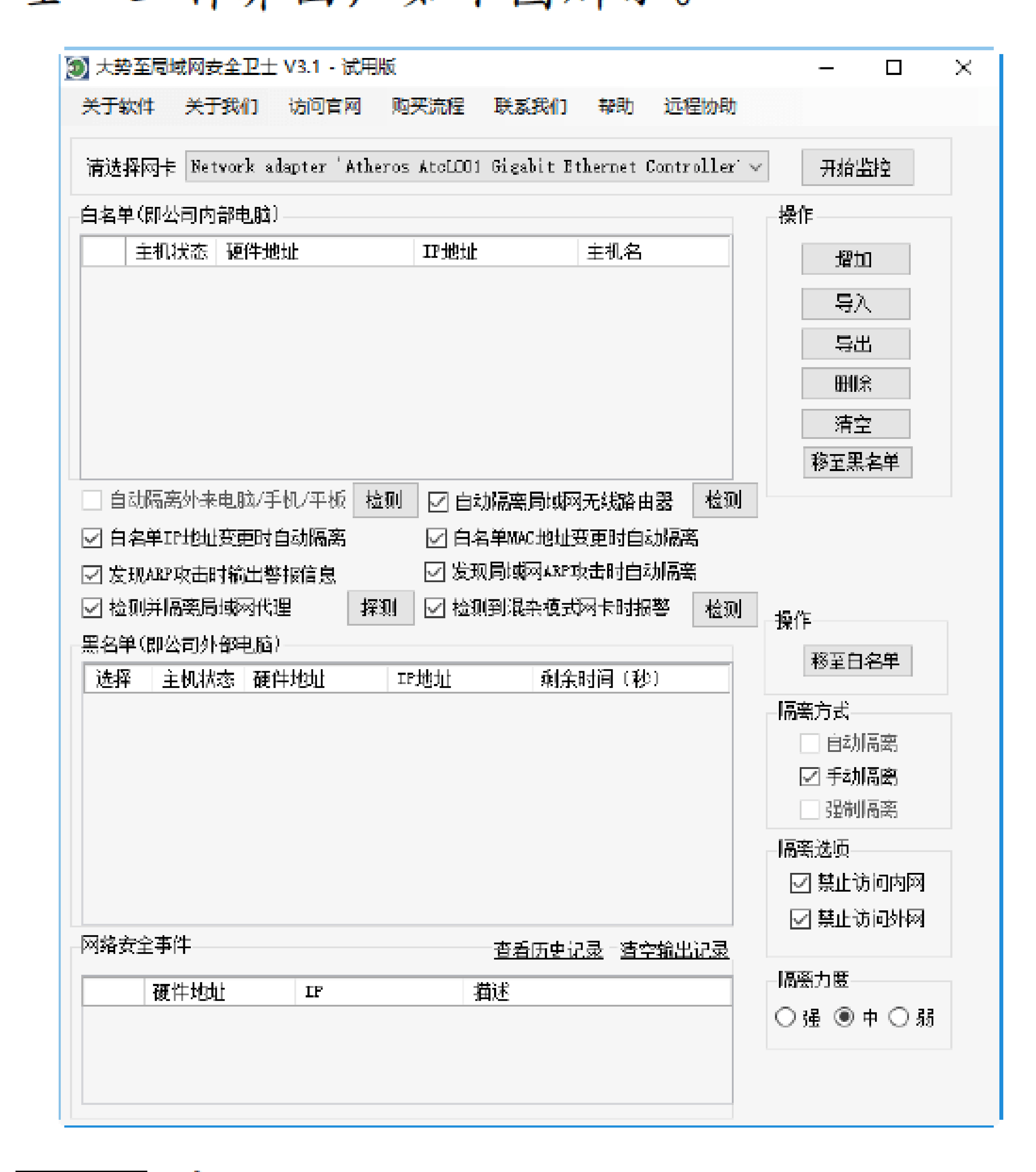


实战9：使用“大势至局域网安全卫士”保护局域网

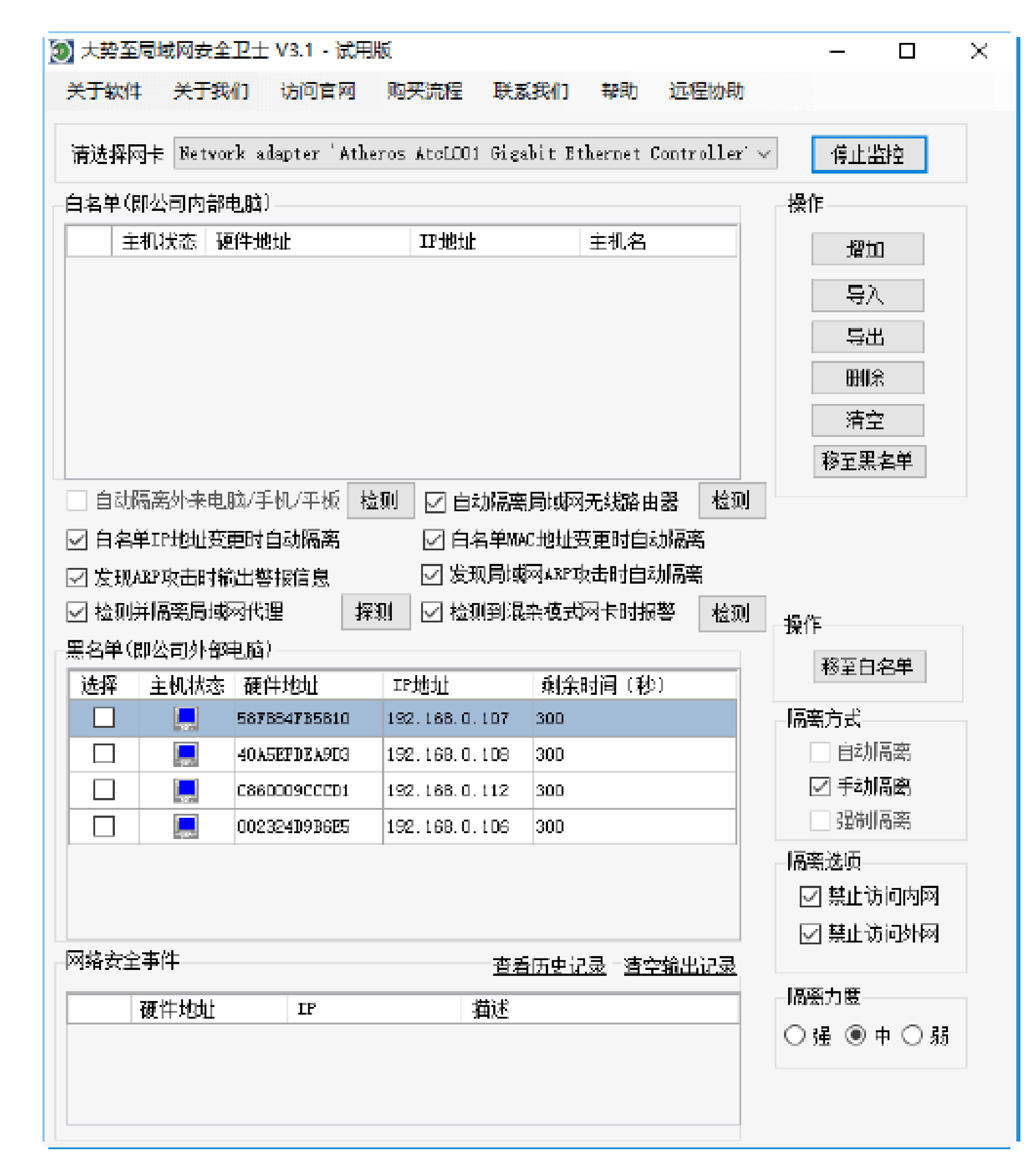
“大势至局域网安全卫士”是一款专业的局域网安全防护系统，它能够有效地防止外来计算机接入公司局域网、有效隔离局域网计算机，并且还有禁止计算机修改IP和MAC地址、检测局域网混杂模式网卡、防御局域网ARP攻击等功能。

使用“大势至局域网安全卫士”防护系统安全的操作步骤如下。

Step 01 下载并安装“大势至局域网安全卫士”，即可打开“大势至局域网安全卫士”工作界面，如下图所示。



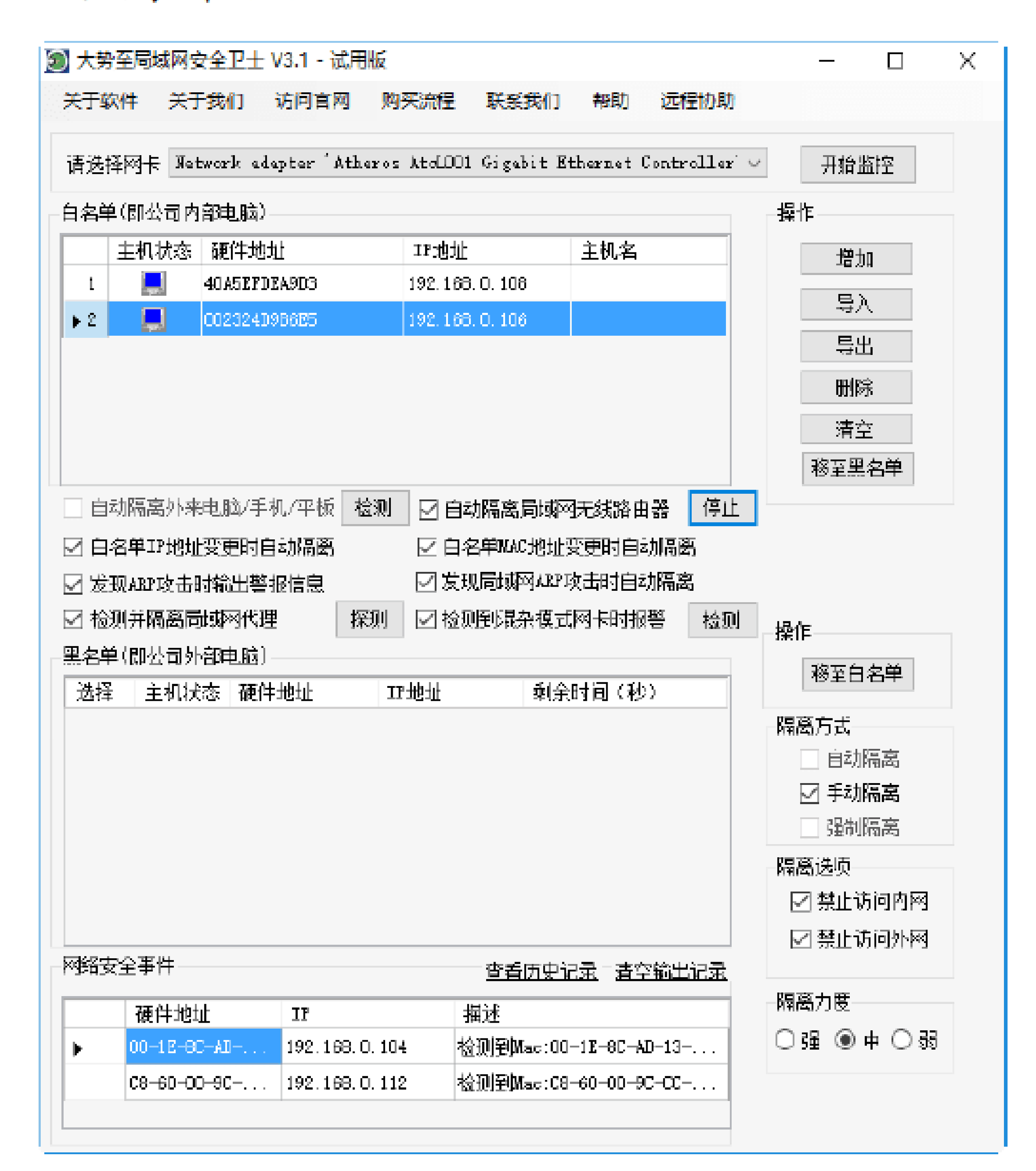
Step 02 单击“开始监控”按钮，即可开始监控当前局域网中的计算机信息，对于局域网外的计算机将显示在“黑名单”窗格之中，如下图所示。



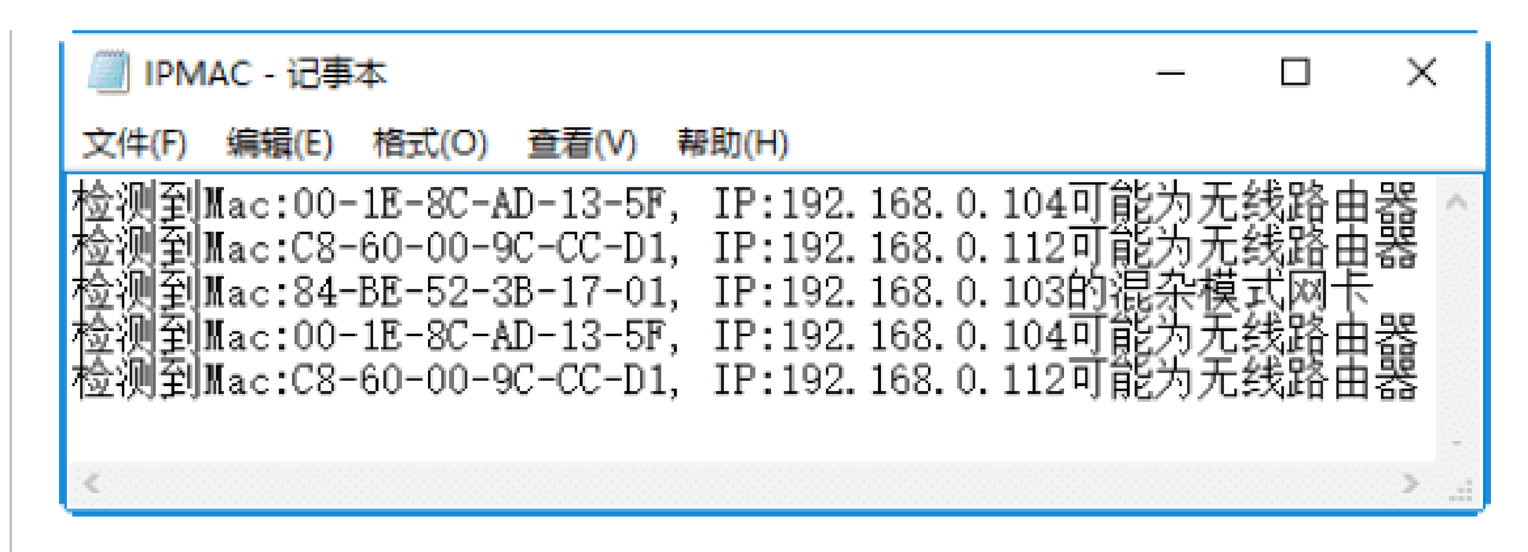
Step 03 如果确定某台计算机是局域网内的计算机，则可以在“黑名单”窗格中选中该计算机信息，然后单击“移至白名单”按钮，将其移动到“白名单”窗格之中，如下图所示。



Step 04 单击“自动隔离局域网无线路由器”右侧的“检测”按钮，可以检测当前局域网中存在的无线路由器设备信息，并在“网络安全事件”窗格中显示检测结果，如下图所示。



Step 05 单击“查看历史记录”按钮，即可打开“IPMAC-记事本”窗口，在其中查看检测结果，如下图所示。



“大势至局域网安全卫士”常用功能介绍如下。

（1）“自动隔离外来计算机/手机/平板”复选框：禁止外部计算机（如笔记本）或移动设备（如平板计算机或手机）接入单位局域网访问因特网。

（2）“自动隔离局域网无线路由器”复选框：当检测到局域网中存在无线路由器时，自动将其隔离。

（3）“白名单IP地址变更时自动隔离”复选框：禁止单位内部计算机修改IP地址，防止IP地址盗用、IP冲突攻击、越权上网或逃避网络监控。

（4）“白名单MAC地址变更时自动隔离”复选框：禁止单位内部计算机修改MAC地址。

（5）“发现ARP攻击时输出报警信息”复选框：当发现ARP攻击时，输出报警信息。

（6）“发现局域网ARP攻击时自动隔离”复选框：当检测到局域网中存在ARP攻击时，自动将发出ARP攻击的计算机隔离。

（7）“检测并隔离局域网代理”复选框：检测局域网中是否存在代理服务器，一旦检测到就会将其隔离。

（8）“检测到混杂模式网卡时报警”复选框：检测局域网内处于混杂模式的网卡，防止局域网计算机运行黑客软件、嗅探软件、抓包软件等，给出报警信息。

9.5　实战演练

实战演练1——设置局域网中宽带连接方式



当申请ADSL服务后，当地ISP员工会主动上门安装ADSL MODEM并配置好上网

设置，进而安装网络拨号程序，设置上网客户端。ADSL的拨号软件有很多，但使用最多的还是Windows系统自带的拨号程序，即宽带连接。设置局域网中宽带连接方式的操作步骤如下。

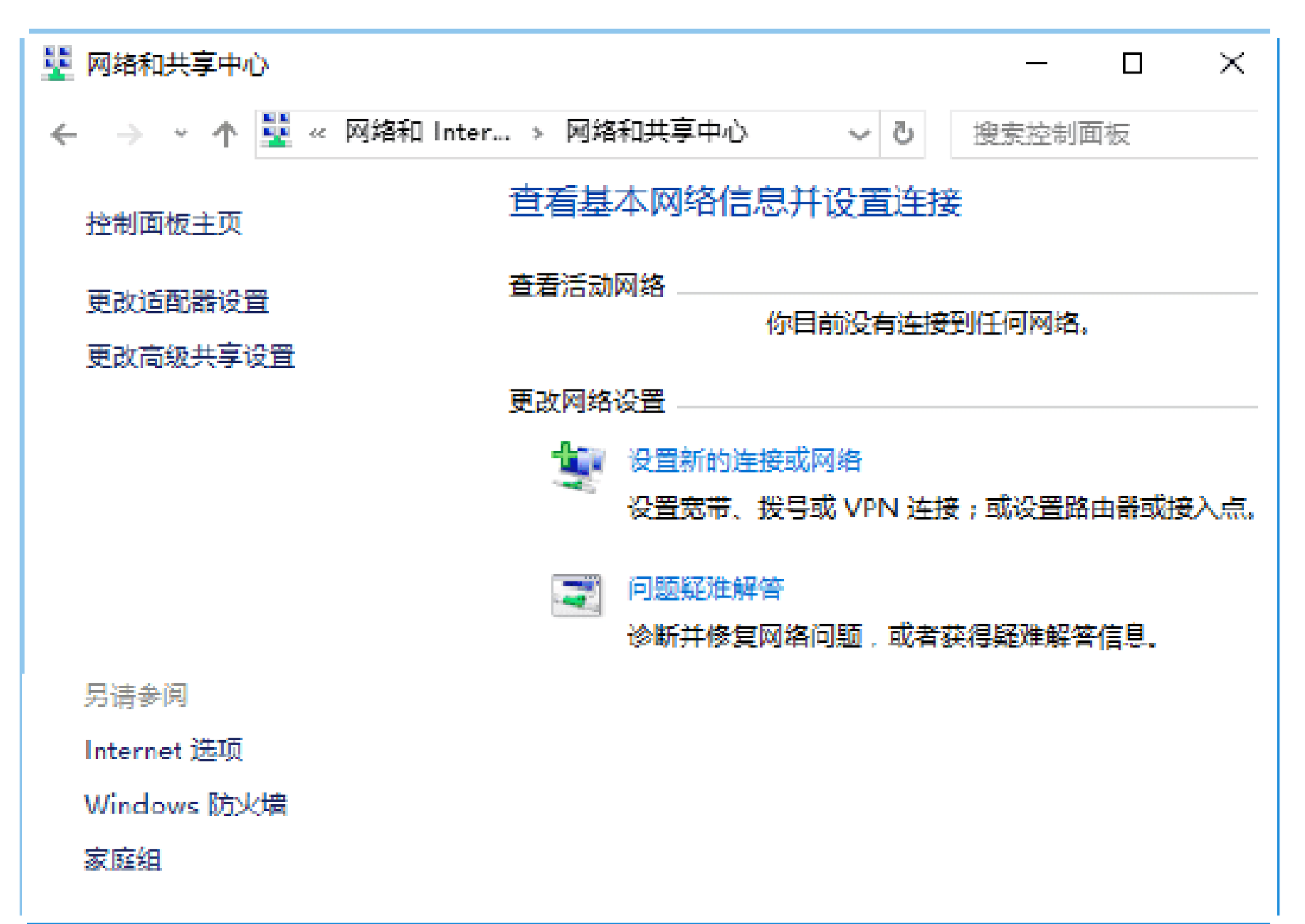
Step 01 单击“开始”按钮，在打开的“开始”面板中选择“控制面板”选项，即可打开“控制面板”窗口，如下图所示。



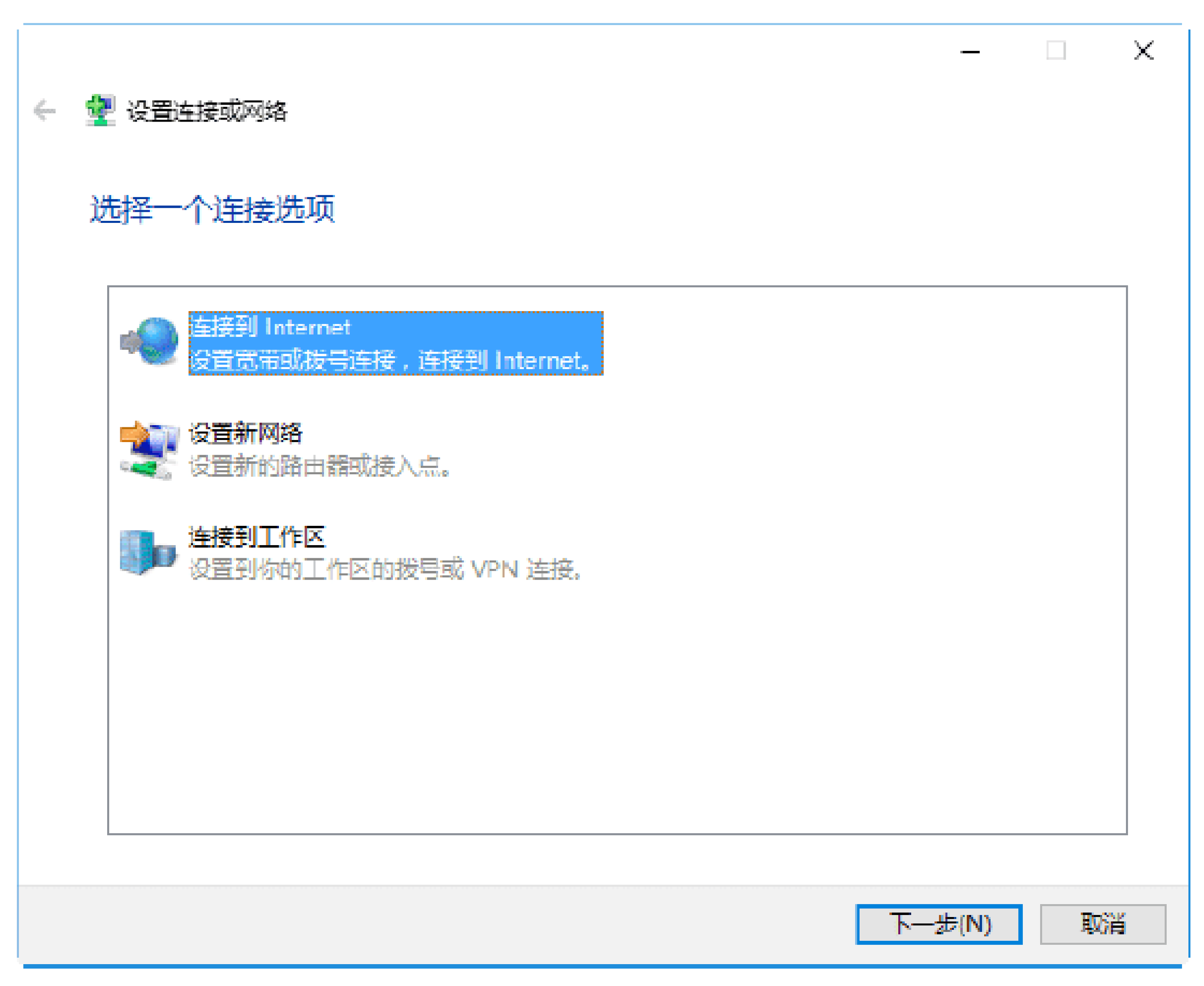
Step 02 单击“网络和Internet”选项，即可打开“网络和Internet”窗口，如下图所示。



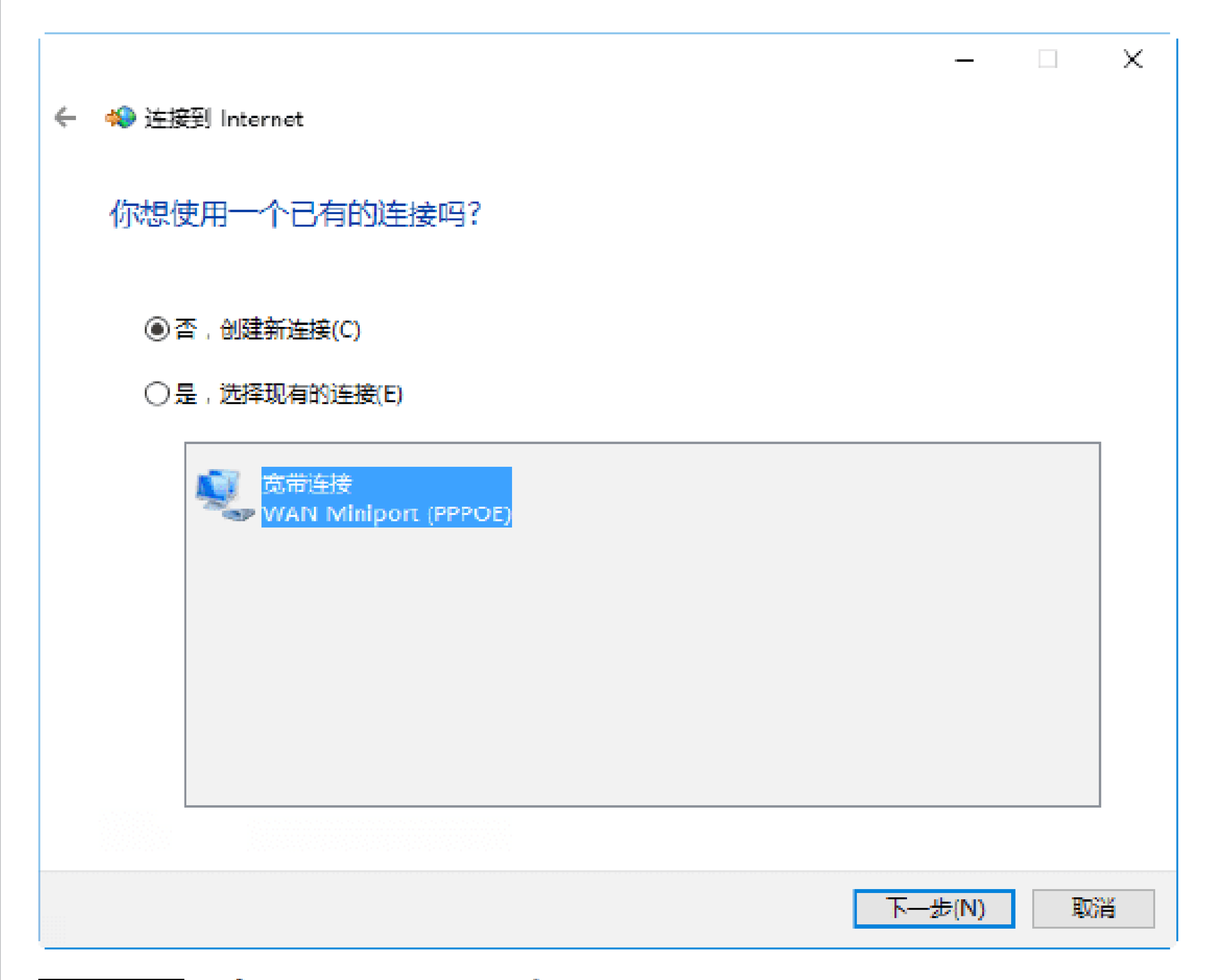
Step 03 选择“网络和共享中心”选项，即可打开“网络和共享中心”窗口，在其中用户可以查看本机系统的基本网络信息，如下图所示。



Step 04 在“更改网络设置”区域中单击“设置新的连接或网络”超级链接，即可打开“设置连接或网络”对话框，在其中选择“连接到Internet”选项，如下图所示。



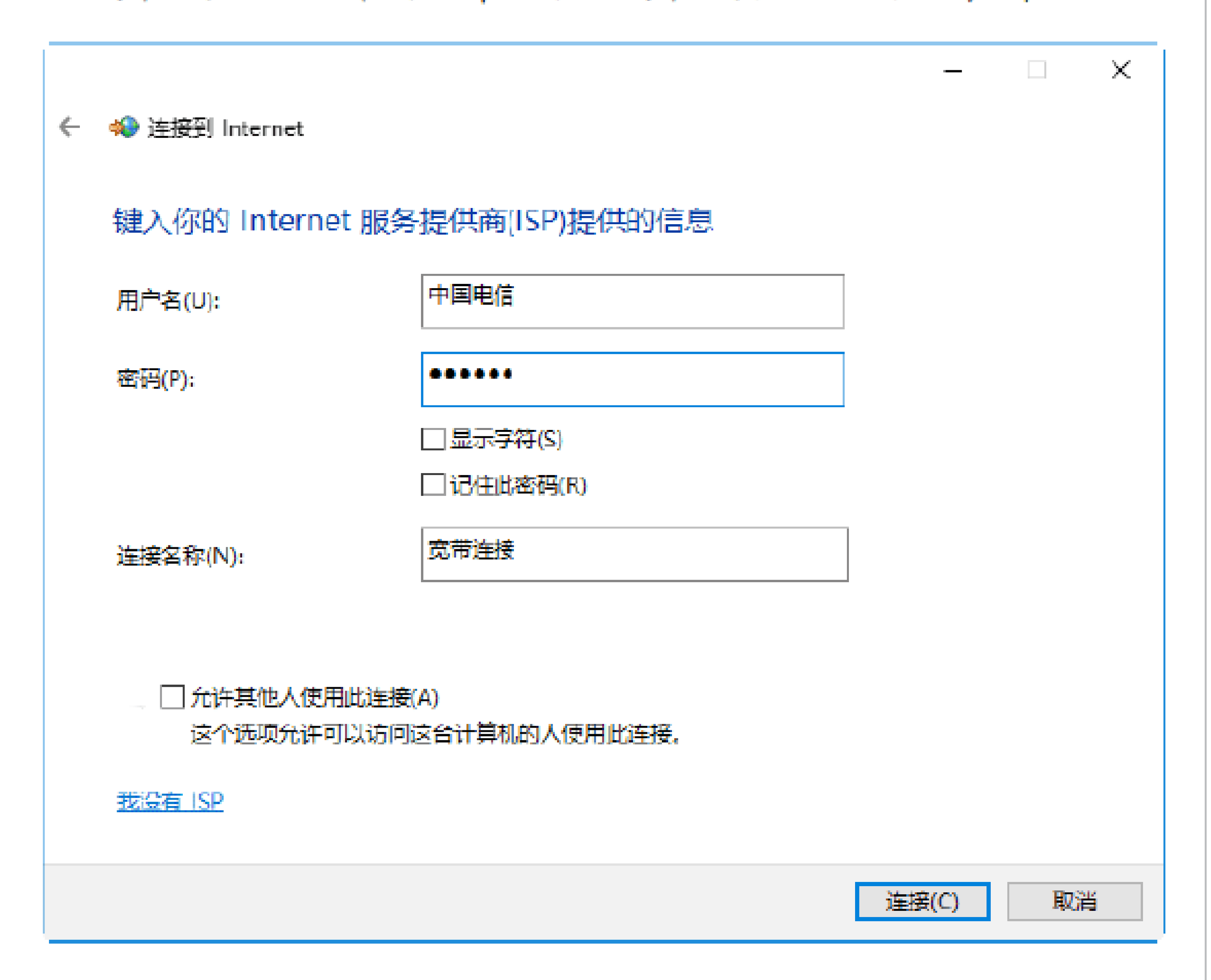
Step 05 单击“下一步”按钮，即可打开“你想使用一个已有的连接吗？”对话框，在其中选中“否，创建新连接”单选按钮，如下图所示。



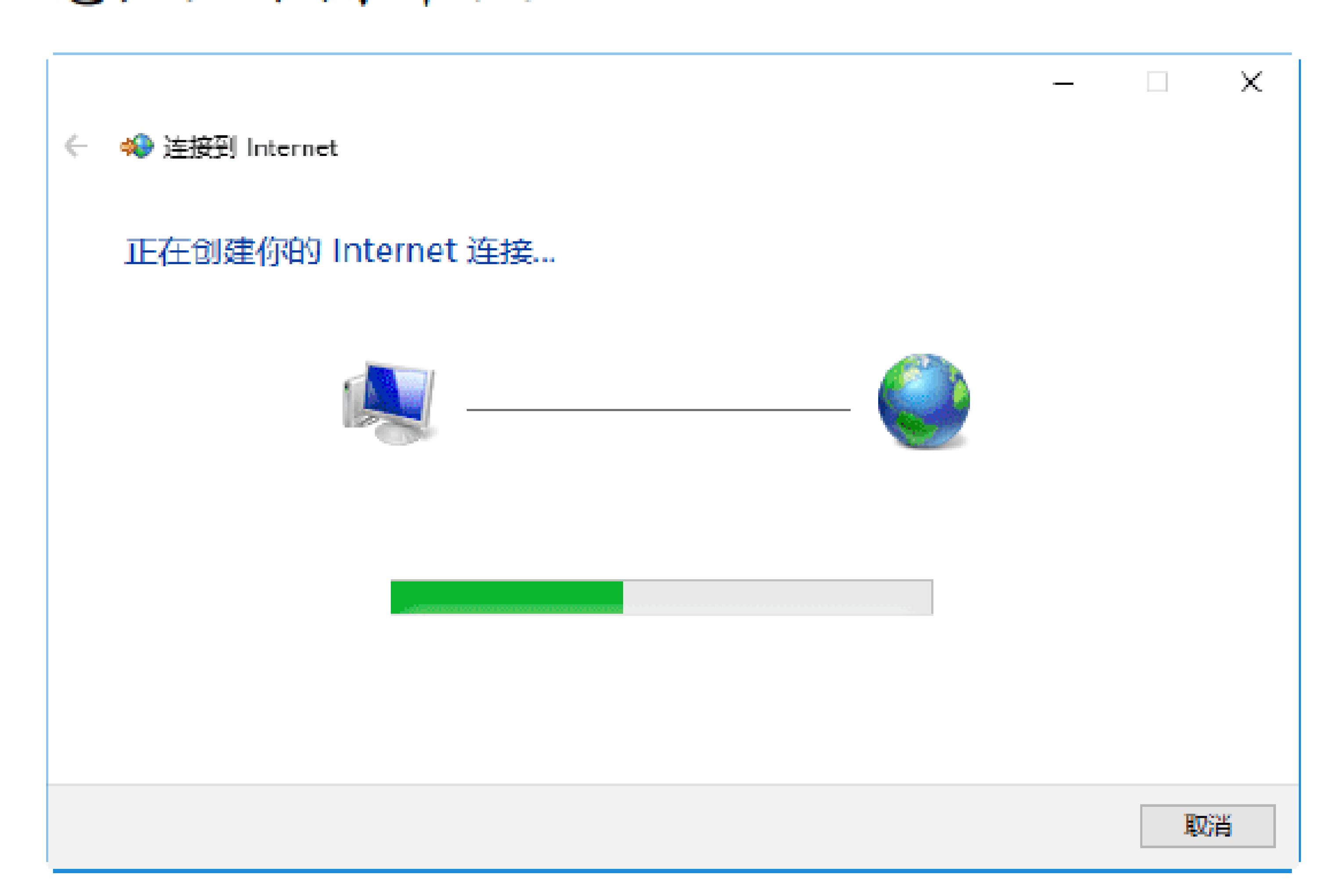
Step 06 单击“下一步”按钮，即可打开“你希望如何连接？”对话框，如下图所示。



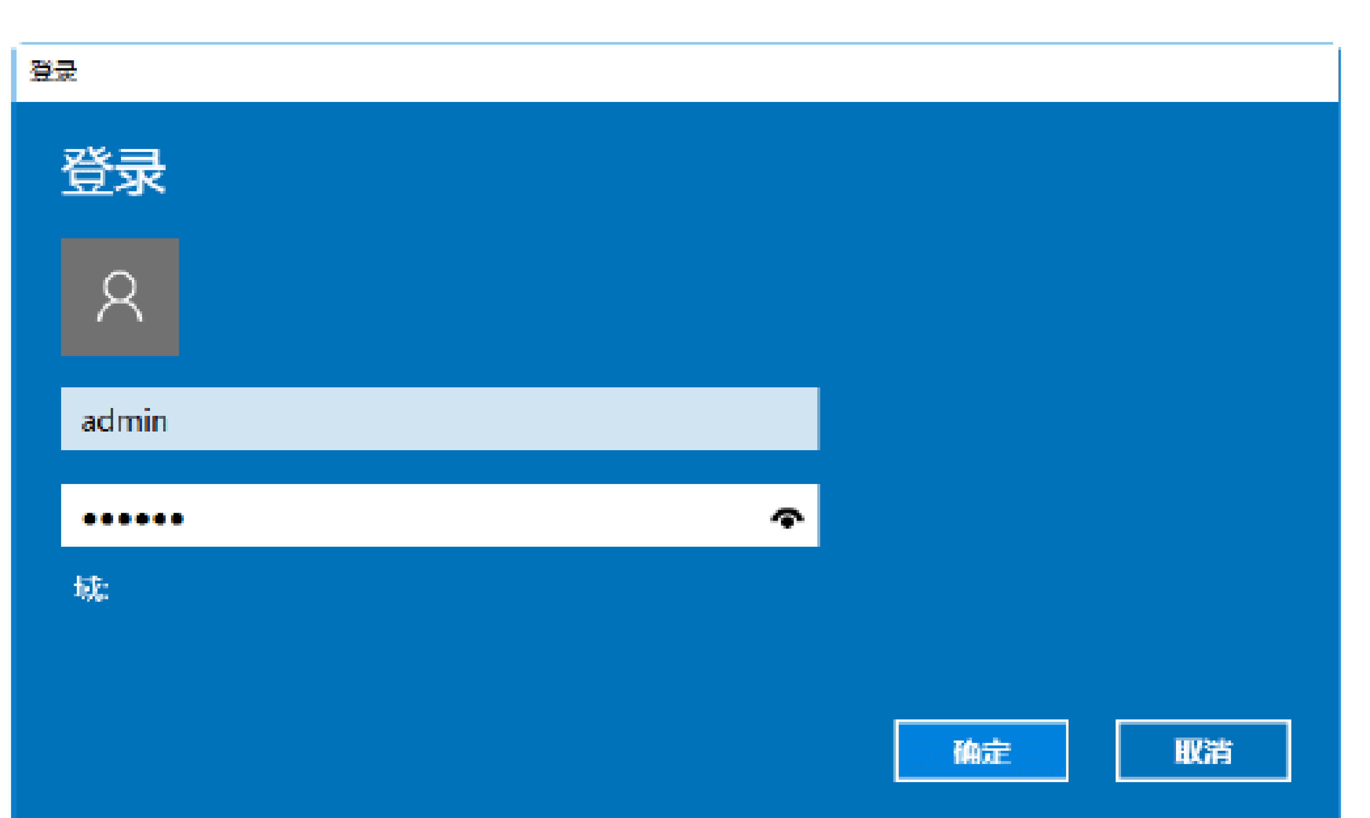
Step 07 单击“宽带（PPPoE）（R）”链接，即可打开“键入你的Internet服务提供商（ISP）提供的信息”对话框，在“用户名”文本框中输入服务提供商的名字，在“密码”文本框中输入密码，如下图所示。



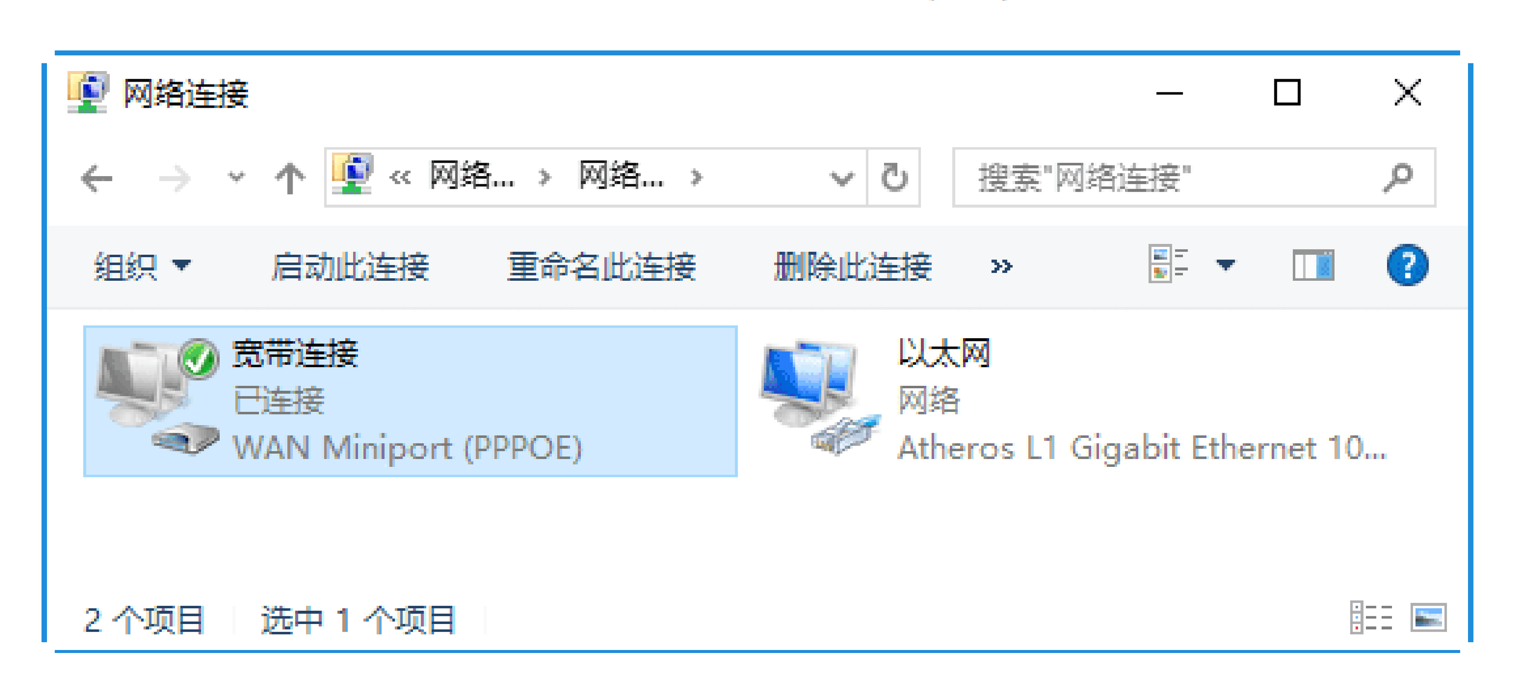
Step 08 单击“连接”按钮，即可打开“连接到Internet”对话框，提示用户正在连接到宽带，并显示正在验证用户名和密码等信息，如下图所示。



Step 09 等待验证用户名和密码完毕后，如果正确，则弹出“登录”对话框。在“用户名”和“密码”文本框中输入服务商提供的用户名和密码，如下图所示。



Step 10 单击“确定”按钮，即可成功连接，在“网络和共享中心”窗口中选择“更改适配器设置”选项，即可打开“网络连接”窗口，在其中可以看到“宽带连接”呈现已连接的状态，如下图所示。



Step 11 在桌面上双击“IE浏览器”图标，即可打开IE浏览器窗口，并打开当前设置的首页——百度首页，如下图所示。



Step 12 在百度“搜索”文本框中输入需要搜索内容，如“新闻”，单击“百度一下”按钮，即可打开搜索有关新闻的相关网页，则表明目前的计算机已经与外网联通，如下图所示。

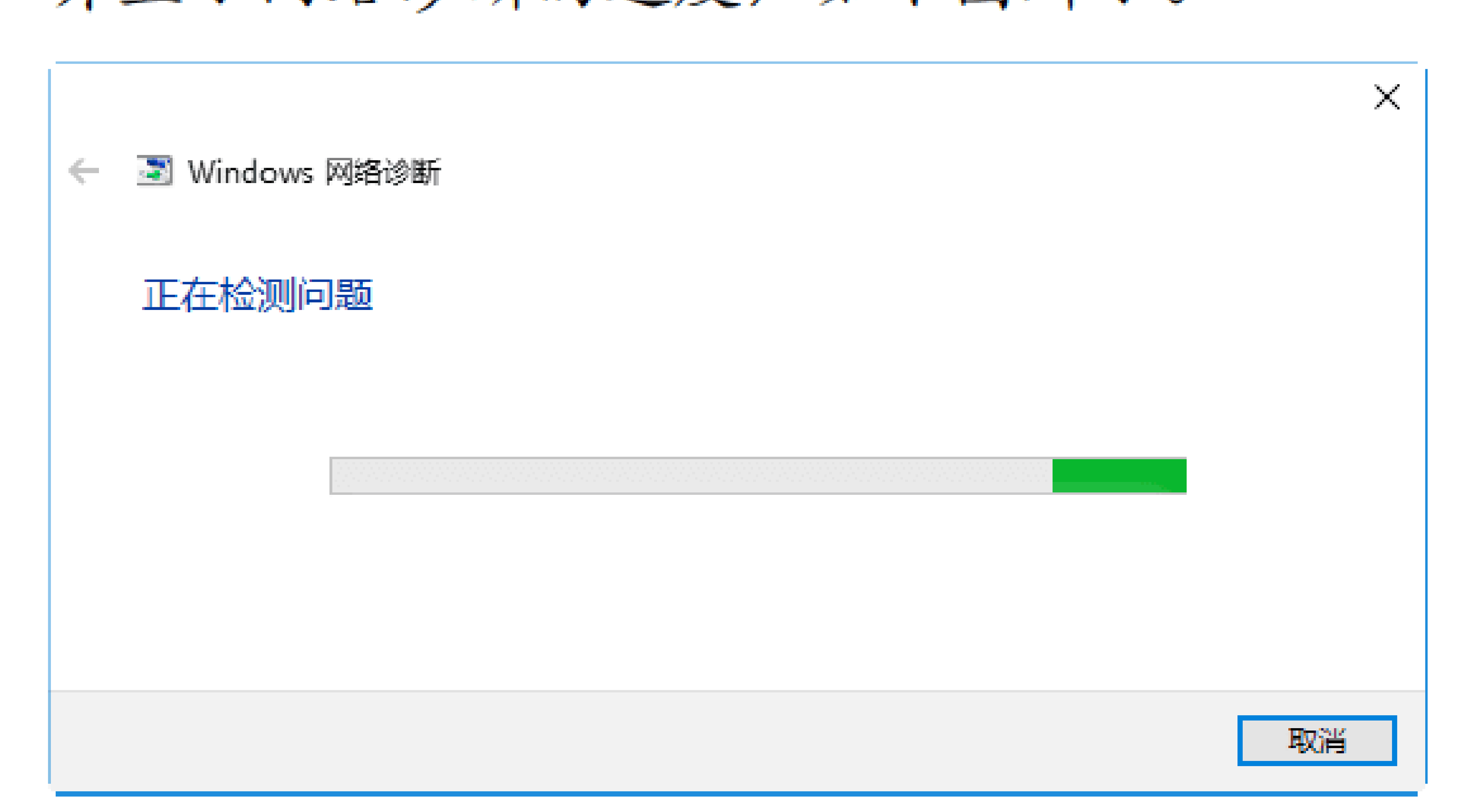




实战演练2——诊断和修复网络不通的问题

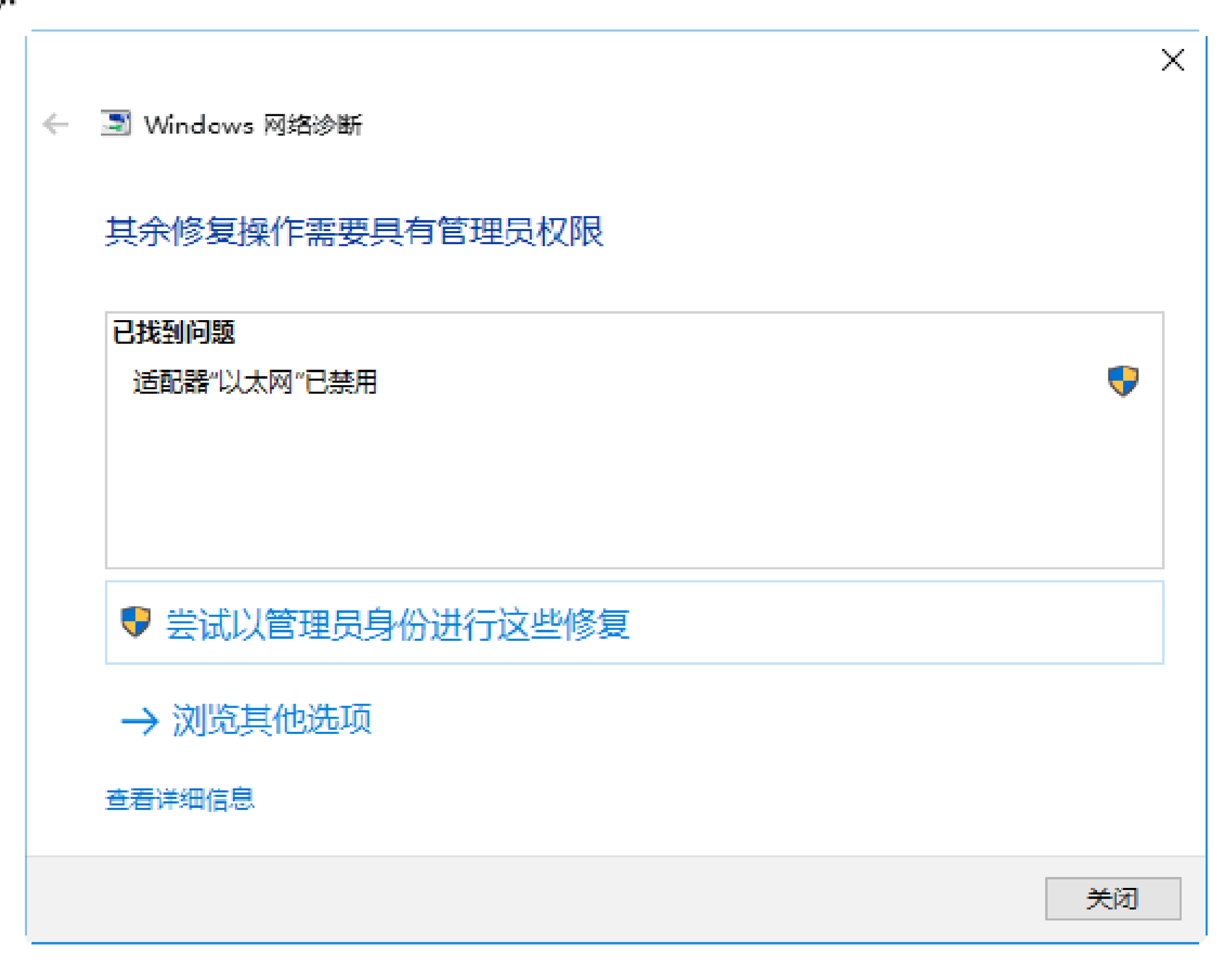
当自己的计算机不能上网时，说明计算机与网络连接不通，这时就需要诊断和修复网络了。具体的操作步骤如下。

Step 01 打开“网络连接”窗口，右击需要诊断的网络图标，在弹出的快捷菜单中选择“诊断”选项，弹出“Windows网络诊断”窗口，并显示网络诊断的进度，如下图所示。

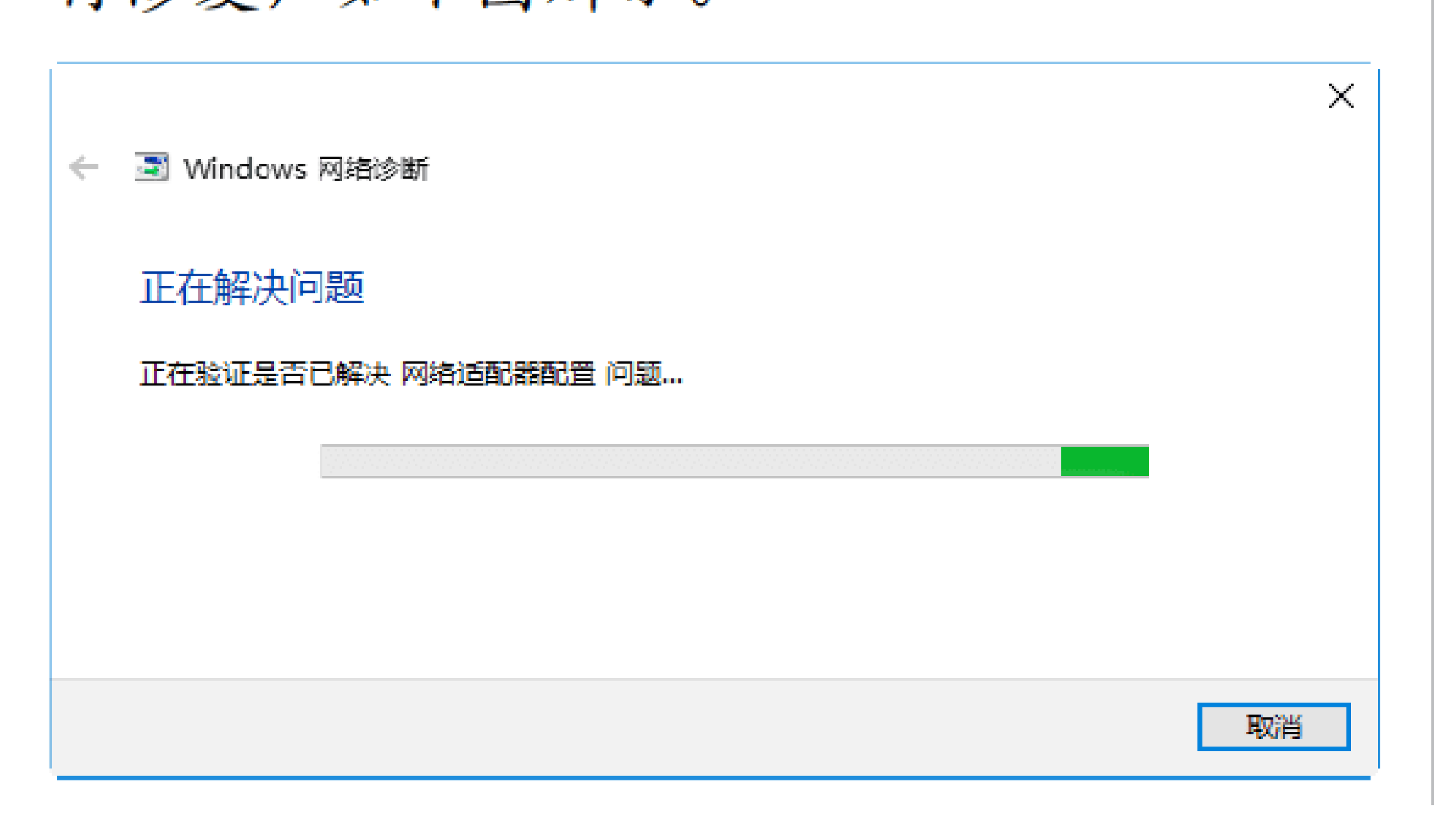




Step 02 诊断完成后，将会在下方的窗格中显示诊断的结果，如下图所示。



Step 03 单击“尝试以管理员身份进行这些修复”链接，即可开始对诊断出来的问题进行修复，如下图所示。



Step 04 修复完毕后，会给出修复的结果，提示用户疑难解答已经完成，并在下方显示已修复信息提示，如下图所示。

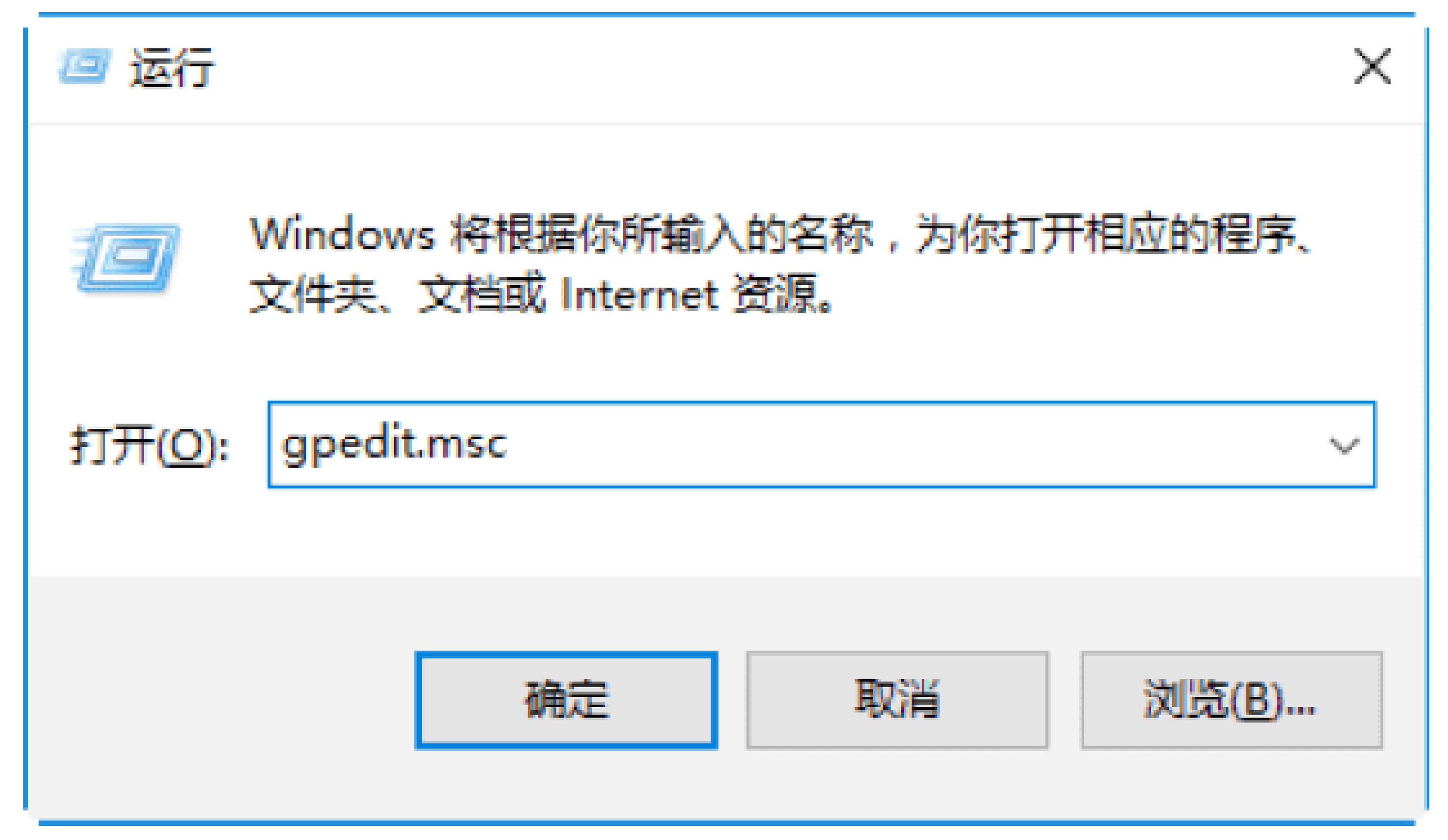


9.6　小试身手

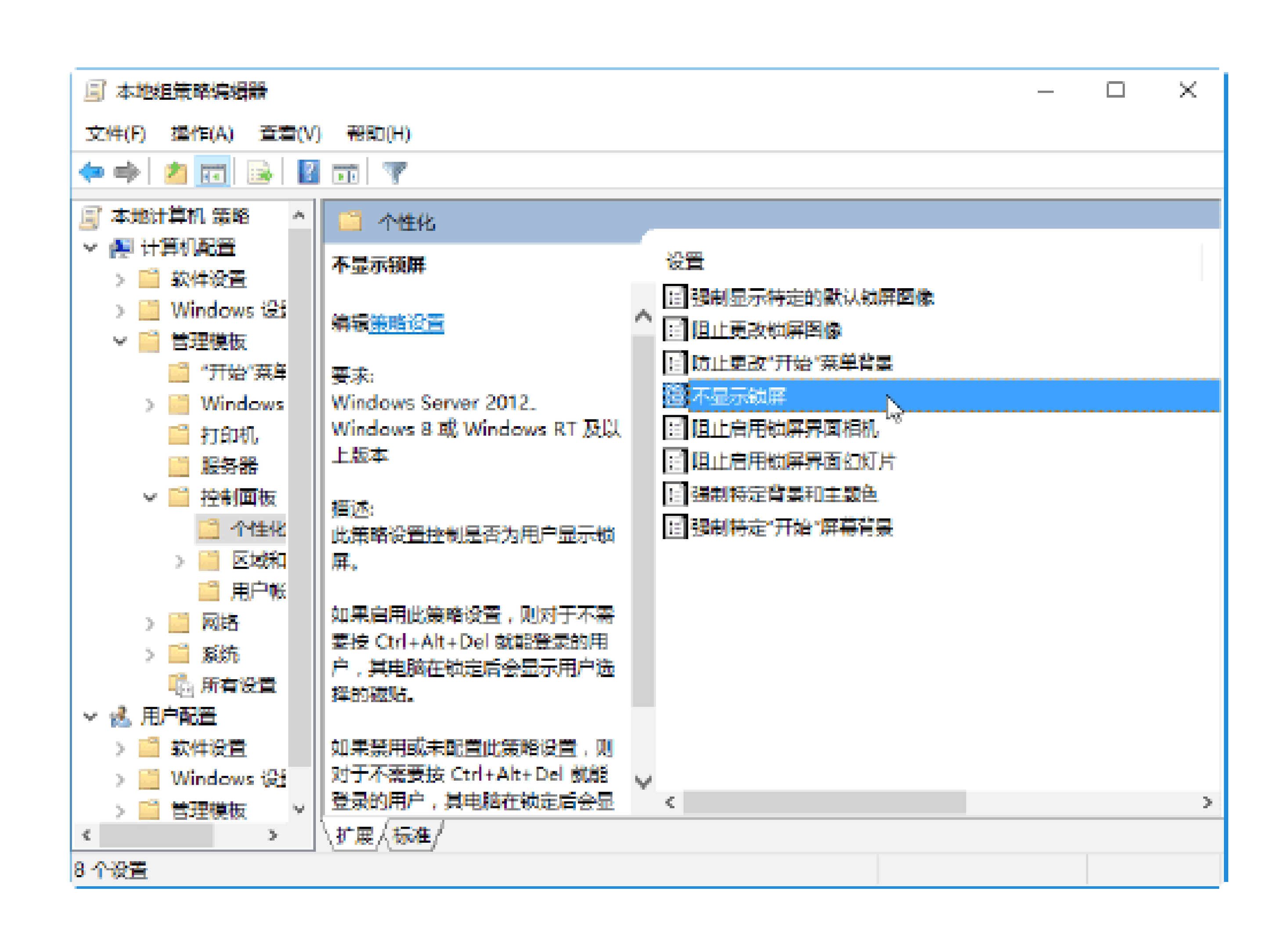
练习1：取消计算机的开机锁屏界面

计算机的开机锁屏界面会给人以绚丽的视觉效果，但会影响开机的时间和速度，用户可以根据需要取消系统启动后的锁屏界面。具体的操作步骤如下。

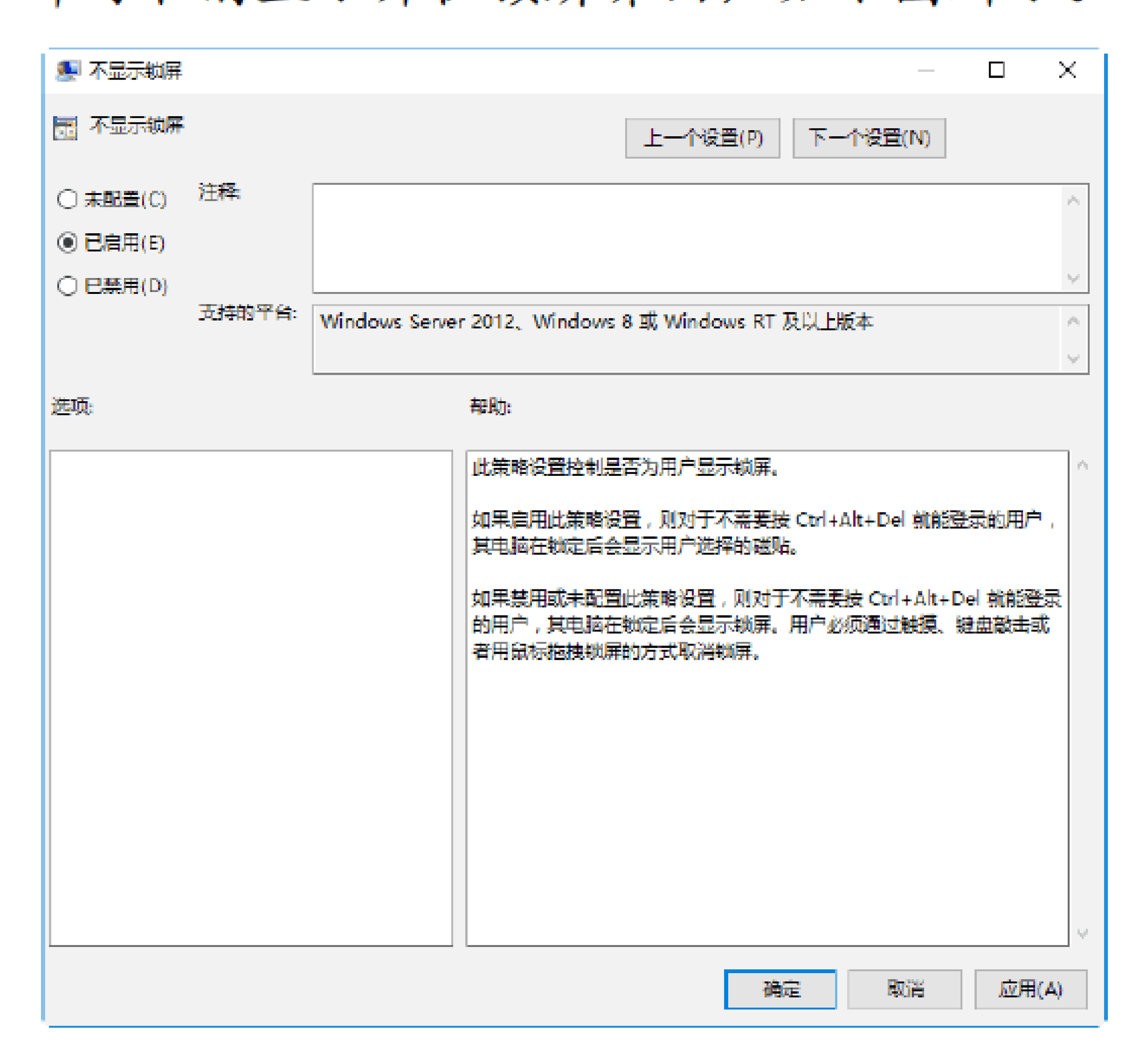
Step 01 按WIN+R组合键，打开“运行”对话框，输入gpedit.msc命令，如下图所示，按Enter键或单击“确定”按钮。



Step 02 打开“本地组策略编辑器”窗口，选择“计算机配置”→“管理模板”→“控制面板”→“个性化”选项，在“设置”列表中双击“不显示锁屏”选项，如下图所示。



Step 03 打开“不显示锁屏”对话框，选中“已启用”单选按钮，单击“确定”按钮，即可取消显示开机锁屏界面，如下图所示。



练习2：我用左手使用鼠标怎么办？

通过对鼠标键的设置，可以使鼠标适应左手用鼠标用户的使用习惯。具体的操作步骤如下。

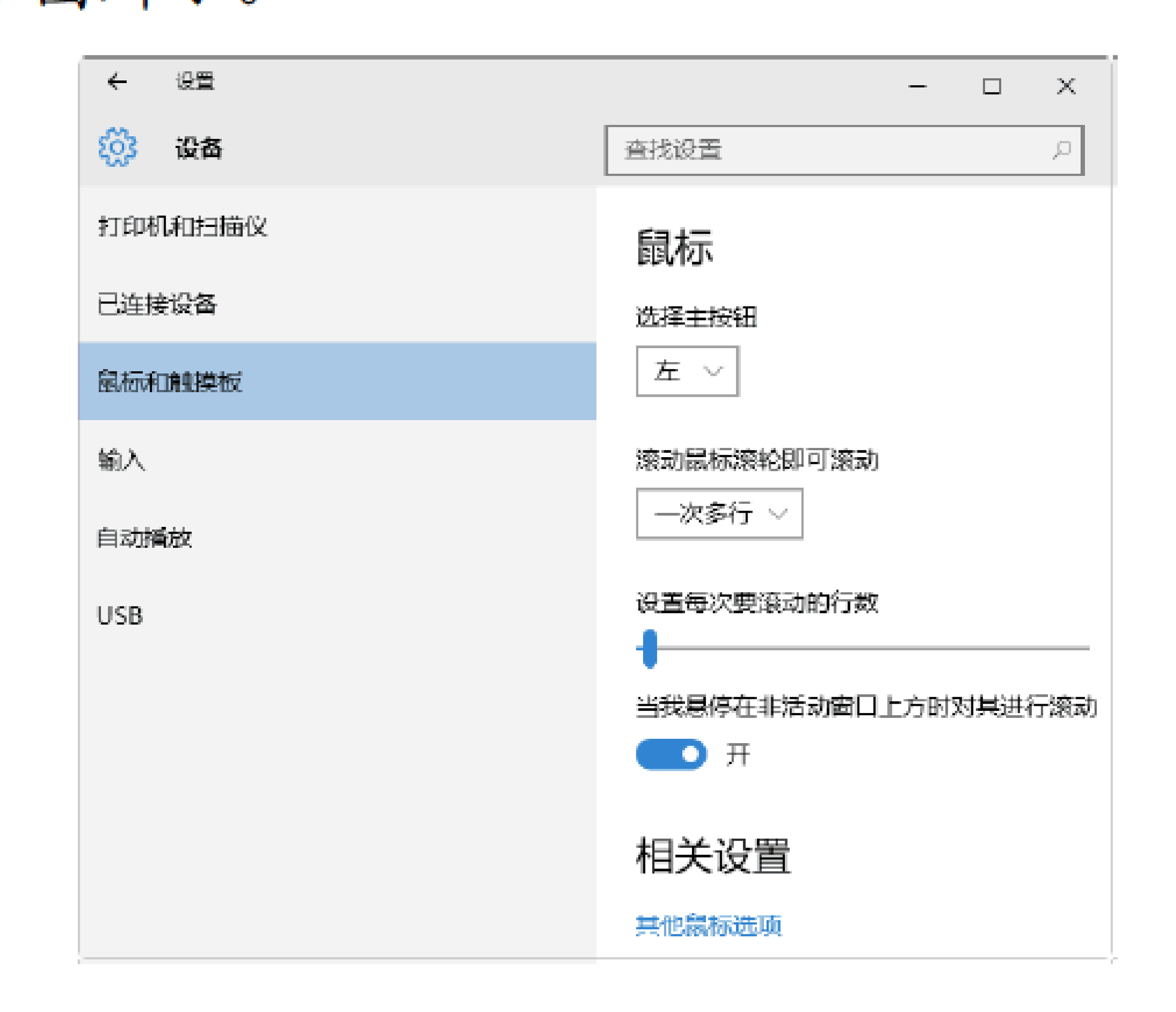
Step 01 单击“开始”按钮，在弹出的菜单中选择“设置”选项。



Step 02 弹出“设置”窗口，选择“设备”选项，如下图所示。

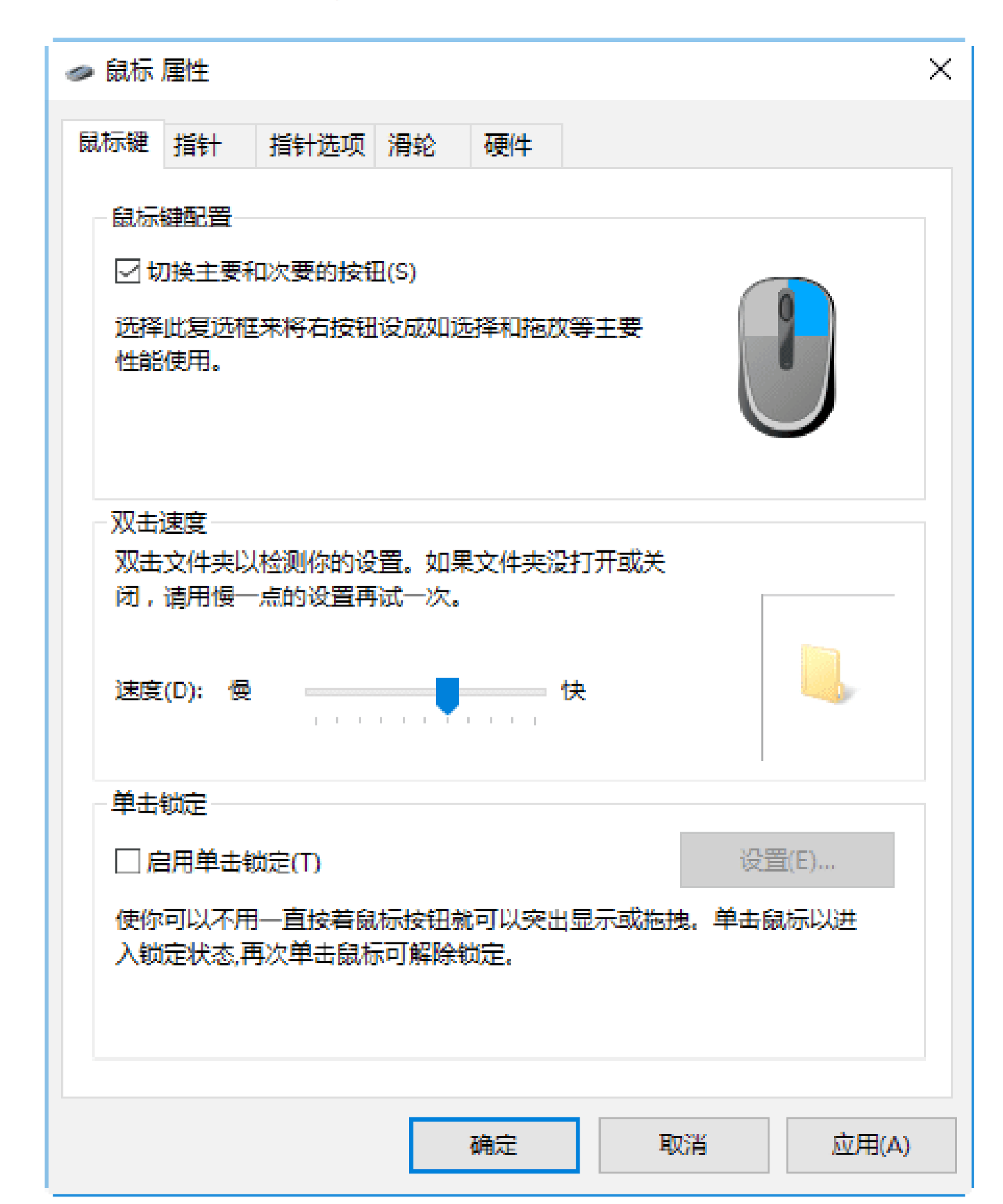


Step 03 弹出“设置”窗口，在左侧的列表中选择“鼠标和触摸板”选项，然后在右侧窗口中选择“其他鼠标选项”超链接，如下图所示。



Step 04 弹出“鼠标 属性”对话框，选择“鼠标键”选项卡，然后勾选“切换主要和次要的按钮”复选框，如下图所示，单击“确定”按钮即可完成设置。





第10章　无线局域网的安全防护

无线网络是利用电磁波作为数据传输的媒介，就应用层面而言，与有线网络的用途完全相似，最大的不同是传输信息的媒介不同。本章介绍无线网络安全的防护，主要内容包括组建无线局域网、共享无线上网、无线网络的安全防护、无线路由器的管理工具等。

10.1　认识无线局域网

无线局域网是通过无线通信技术进行组网的一个结合产物，它采用无线电波、红外线或激光，通过无线通信传输媒介代替传统网线，构成传统局域网的功能，能够使用户随时、随地进行上网。

10.1.1　无线局域网的优点

与传统有线局域网相比，无线局域网具有如下优点：

（1）灵活性。在有线局域网中，网络设备的安放位置受到网络位置的限制，而无线局域网则没有，只要信号覆盖范围内的任何位置都可以接入网络。

（2）移动性。无线局域网的最大优点在于它的移动性，接入的用户可以在覆盖范围内随意移动，且还能保持网络的连接。

（3）方便安装。无线局域网可以最大程度地减少网络布线，一般只需安装一个或多个接入点设备，便可以建立起一个覆盖面广的网络区域。

（4）方便规划和调整。对于有线局域网而言，办公地点或网络拓扑的改变通常需要重新建网，而无线局域网则可以避免或减少这些情况的发生。

（5）故障定位容易。有线局域网一旦出现物理故障，尤其是由于线路中断或线路不良造成的网络故障，往往很难查找原因，并且线路检修也需要付出很大的代价；无线局域网则不同，故障容易定位，定位后更换故障设备即可恢复网络。

（6）易于扩展。无线局域网有多种配置方式，可以很快从只有几个用户的小型局域网扩展到上千用户的大型网络，并且还有节点间漫游的特性，这些是有线局域网所不能实现的。

10.1.2　无线局域网的缺点

无线局域网的缺点主要体现在性能、速率与安全性三个方面，下面进行详细介绍。

（1）性能。无线局域网是依靠无线电波进行传输的，因此无线电波受到遮挡或者其他电波干扰都可能阻碍电磁波传输，受到这些外因影响会直接导致网络性能降低。

（2）速率。无线信道的传输速率与有线信道相比要低得多，虽然无线局域网还在不断的发展，目前已经能达到最快500Mb/s的传输速率，但是与有线局域网的千兆传输速率还是有差距的。

（3）安全性。由于无线传输的特性导致无线传输是发散的，不要求建立物理连接通道，因此从理论上讲，很容易被监听，造成信息泄露。

10.1.3　认识无线连接方式

WiFi是一种可以将个人计算机、手持设备（如PDA、手机）等终端以无线方式互相连接的技术，并不是无线网络或者是其他无线设备，WiFi是一个无线网络通信技术的品牌，由WiFi联盟（WiFi Alliance）所持有。



以前通过网线连接计算机，自从有了WiFi技术，则可以通过无线电波来连网。常见的无线网络设备就是一个无线路由器，那么在这个无线路由器的电波覆盖的有效范围内，都可以采用WiFi进行联网。如果无线路由器连接了一条ADSL线路或者别的上网线路，则无线路由器又可以被称为一个“热点”。

10.2　组建无线局域网

建立无线局域网的操作比较简单，在有线局域网到户后，用户只需连接一个具有无线WiFi功能的路由器，然后各房间里的计算机、笔记本计算机、手机和iPad等设备利用无线网卡与路由器之间建立无线连接，即可构建一个简单的无线局域网。

实战1：配置无线局域网

建立无线局域网的第一步就是配置无线路由器，默认情况下，具有无线功能的路由器是不开启无线功能的，需要用户手动配置，在开启了路由器的无线功能后，下面就可以配置无线网了。

使用计算机配置无线局域网的操作步骤如下。

Step 01 打开IE浏览器，在地址栏中输入路由器的网址，一般情况下路由器的默认网址为192.168.0.1，输入完毕，单击“转至”按钮，即可打开路由器的登录窗口，如下图所示。



Step 02 在“请输入管理员密码”文本框中输入管理员的密码，默认情况下管理员的密码为123456，如下图所示。



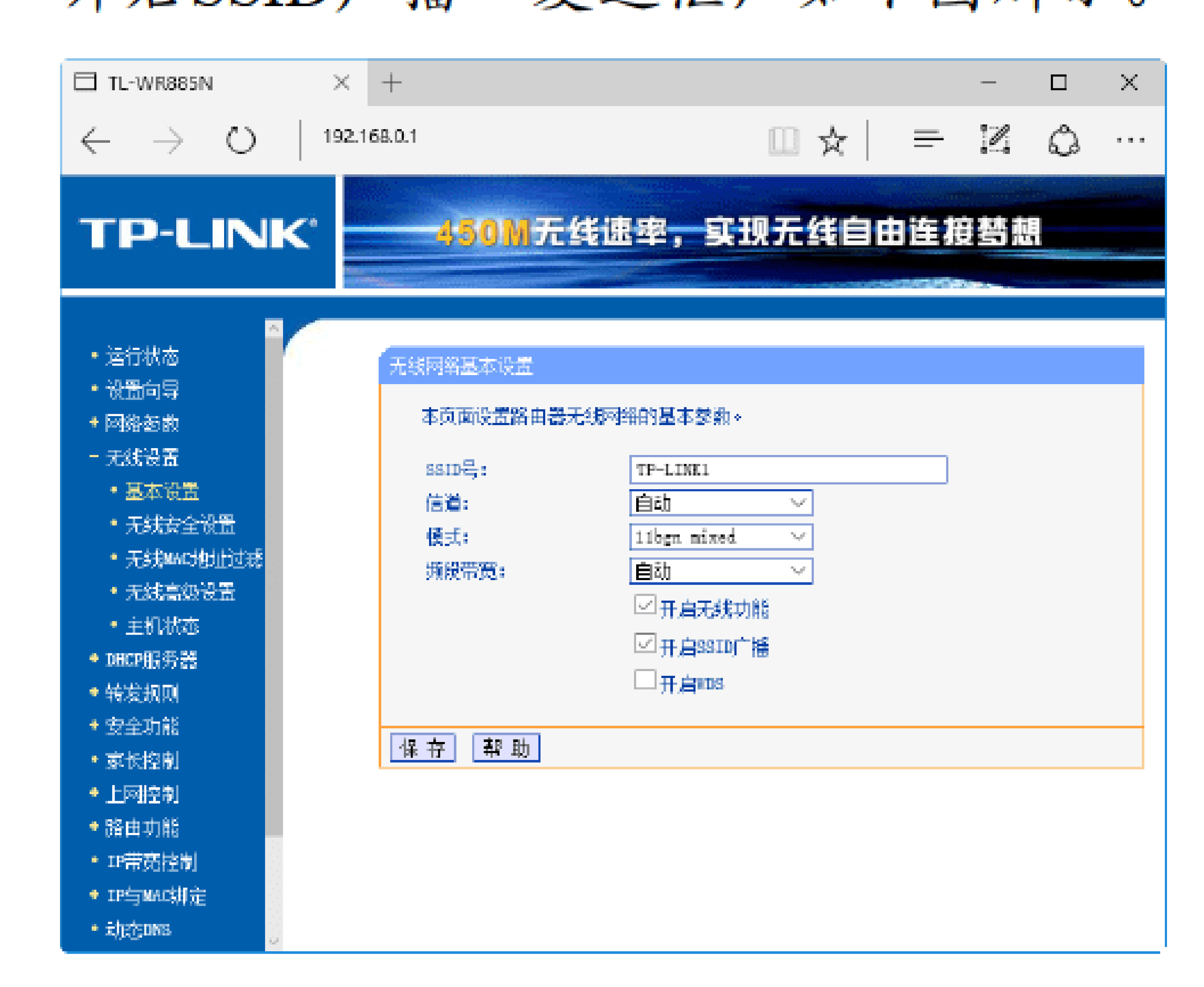
Step 03 单击“确认”按钮，即可进入路由器的“运行状态”工作界面，在其中可以查看路由器的基本信息，如下图所示。





Step 04 选择窗口左侧的“无线设置”选

项，在打开的子选项中选择“基本信息”选项，即可在右侧的窗格中显示无线设置的基本功能，并勾选“开始无线功能”和“开启SSID广播”复选框，如下图所示。

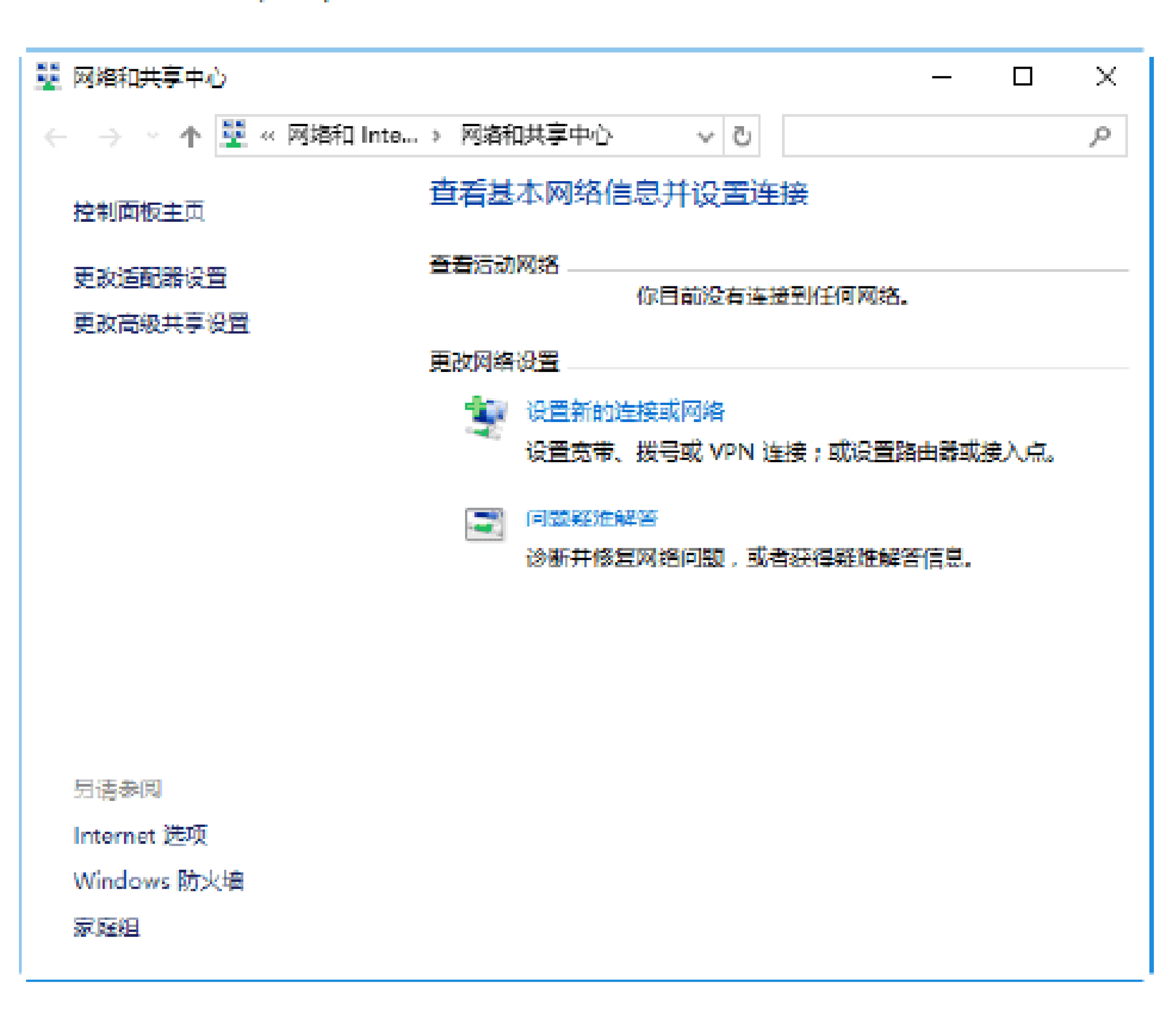


Step 05 当开启了路由器的无线功能后，单击“保存”按钮进行保存，然后重新启动路由器，即可完成无线网的设置，这样具有WiFi功能的手机、计算机、iPad等电子设备就可以与路由器进行无线连接，从而实现共享上网。

实战2：将计算机接入无线局域网

笔记本计算机具有无线接入功能，台式计算机要想接入无线局域网，需要购买相应的无线接收器。这里以笔记本计算机为例，介绍如何将计算机接入无线局域网，具体的操作步骤如下。

Step 01 双击笔记本计算机桌面右下角的无线连接图标，打开“网络和共享中心”窗口，在其中可以看到本台计算机的网络连接状态，如下图所示。



Step 02 单击笔记本计算机桌面右下角的无线连接图标，在打开的界面中显示计算机自动搜索的无线设备和信号，如下图所示。



Step 03 单击一个无线连接设备，展开无线连接功能，在其中勾选“自动连接”复选框，如下图所示。



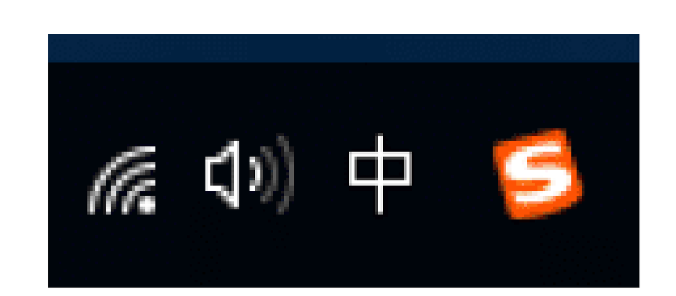
Step 04 单击“连接”按钮，在打开的界面中输入无线连接设备的连接密码，如下图所示。



Step 05 单击“下一步”按钮，开始连接网络，如下图所示。



Step 06 连接到网络之后，桌面右下角的无线连接设备显示正常，并以弧线的方式给出信号的强弱，如下图所示。

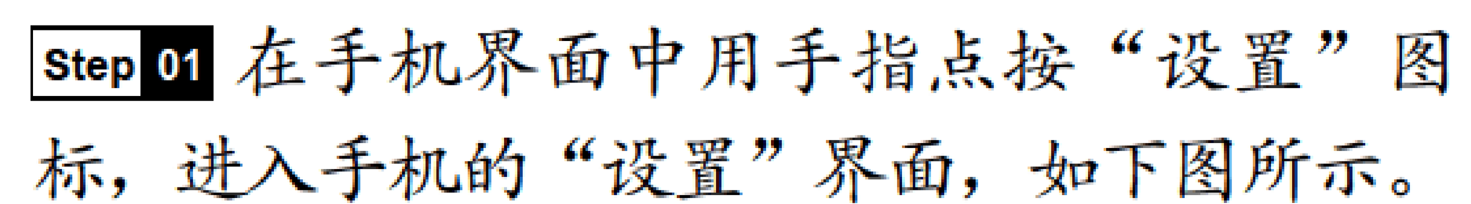


Step 07 再次打开“网络和共享中心”窗口，在其中可以看到这台计算机当前的连接状态，如下图所示。



实战3：将手机接入无线局域网

无线局域网配置完成后，用户可以通过将手机接入WiFi，从而实现无线上网。手机接入WiFi的操作步骤如下。



Step 01 在手机界面中用手指点按“设置”图标，进入手机的“设置”界面，如下图所示。



Step 02 使用手指点按WLAN右侧的“已关闭”，开启手机WLAN功能，并自动搜索周围可用的WLAN，如下图所示。

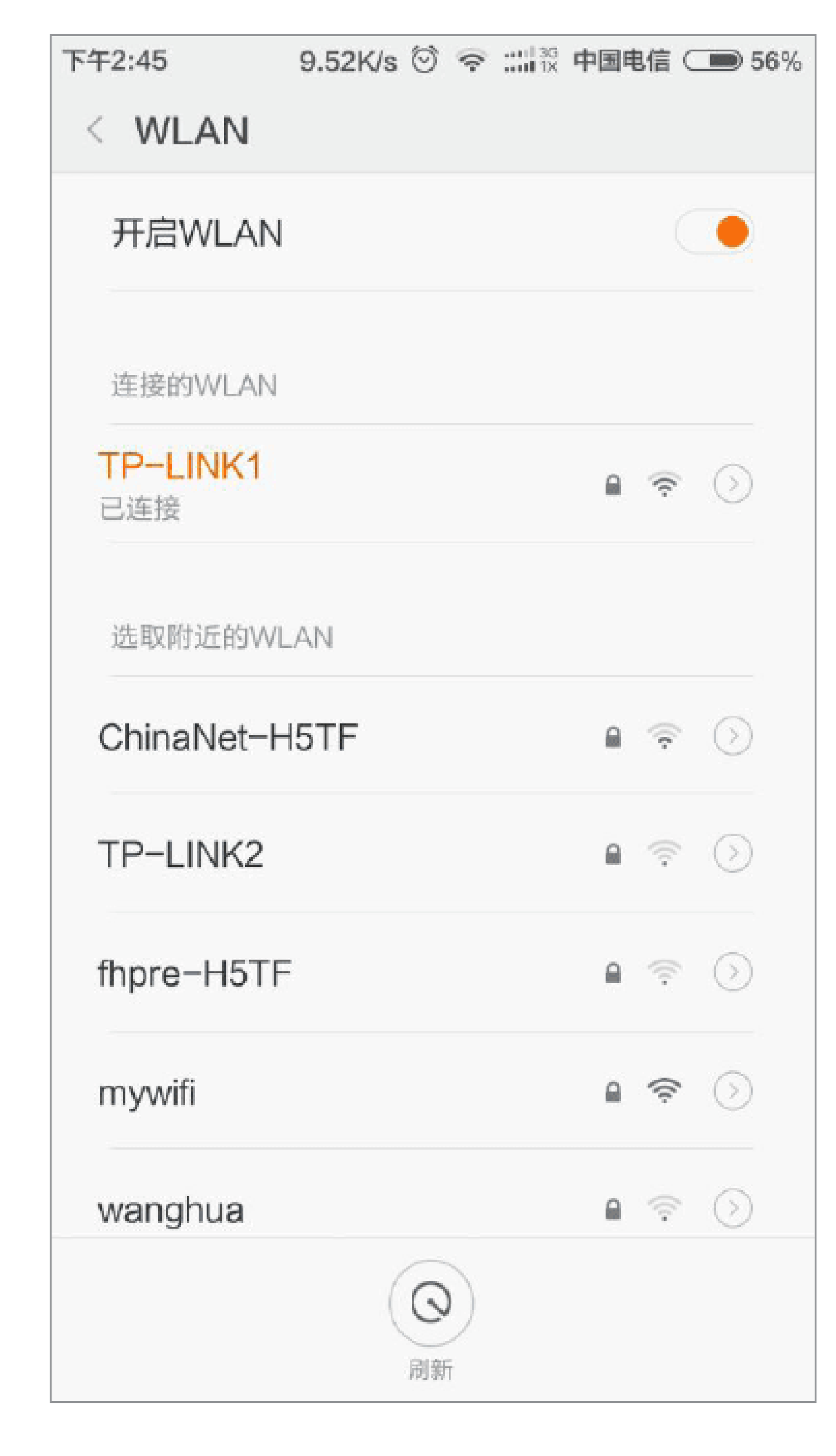




Step 03 使用手指点按可用的WLAN，弹出连接界面，在其中输入相关密码，如下图所示。



Step 04 点按“连接”按钮，即可将手机接入WiFi，并在下方显示“已连接”字样，如下图所示，这样手机就接入WiFi，可以使用手机进行上网了。





10.3 无线局域网的安全设置

无线局域网不需要物理线缆，非常方便，但正因为无线需要靠无线信号进行信息传输，而无线信号又管理不便，因此，数据的安全性更是遭到了前所未有的挑战。于是，各种各样的无线加密算法应运而生。

实战4：设置路由器的管理员密码

路由器的初始密码比较简单，为了保证局域网的安全，一般需要修改或设置管理员密码，具体的操作步骤如下。

Step 01 打开路由器的Web后台设置界面，选择“系统工具”选项下的“修改登录密码”选项，打开“修改管理员密码”工作界面，如下图所示。



Step 02 在“原密码”文本框中输入原来的密码，在“新密码”和“确认新密码”文本框中输入新设置的密码，如下图所示，最后单击“保存”按钮即可。



实战5：设置无线网络WEP密码

WEP采用对称加密机理，数据的加密和解密采用相同的密钥和加密算法。下面详细介绍无线网络WEP加密的具体方法。

1. 设置无线路由器WEP加密数据

Step 01 打开路由器的Web后台设置界面，选择“无线设置”→“无线安全设置”选项，进入“无线网络安全设置”界面，如下图所示。



Step 02 选中WEP单选按钮，在“WEP密钥格式”下拉列表中选择“ASCⅡ码”选项，在“密钥1”后面的“密钥类型”下拉列表中选择“64位”选项，在“密钥内容”文本框中输入要使用的密码，本实例输入密码为cisco，单击“保存”按钮，如下图所示。



2. 客户端连接

需要WEP加密认证的无线客户端连接的具体操作步骤如下。

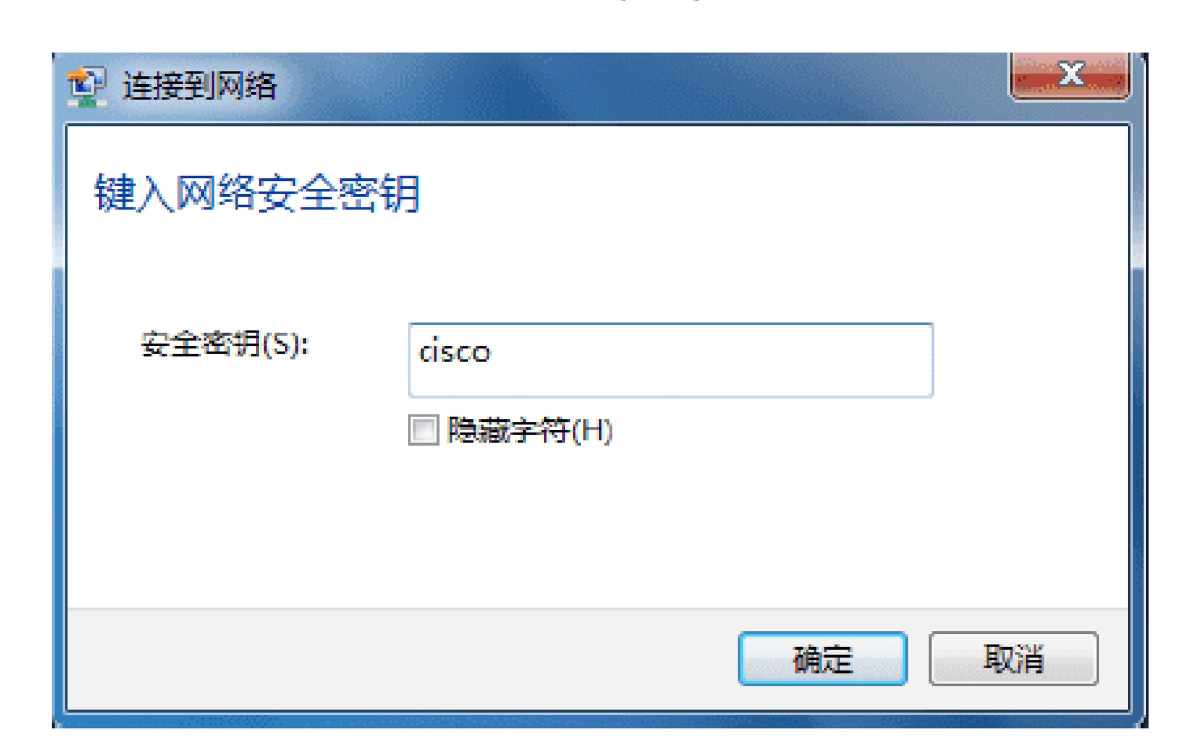
Step 01 单击系统桌面右下角“ ”图标，无线客户端自动扫描到区域内的所有无线信号，如下图所示。



Step 02 右击tp-link信号，在弹出的快捷菜单中选择“连接”选项，如下图所示。



Step 03 弹出“连接到网络”对话框，在“安全密钥”文本框中输入密码cisco，单击“确定”按钮，如下图所示。



Step 04 单击系统桌面右下角“ ”图标，将鼠标放在tp-link信号上，可以看到无线信号的连接情况，如下图所示，表明已经成功连接无线路由器。

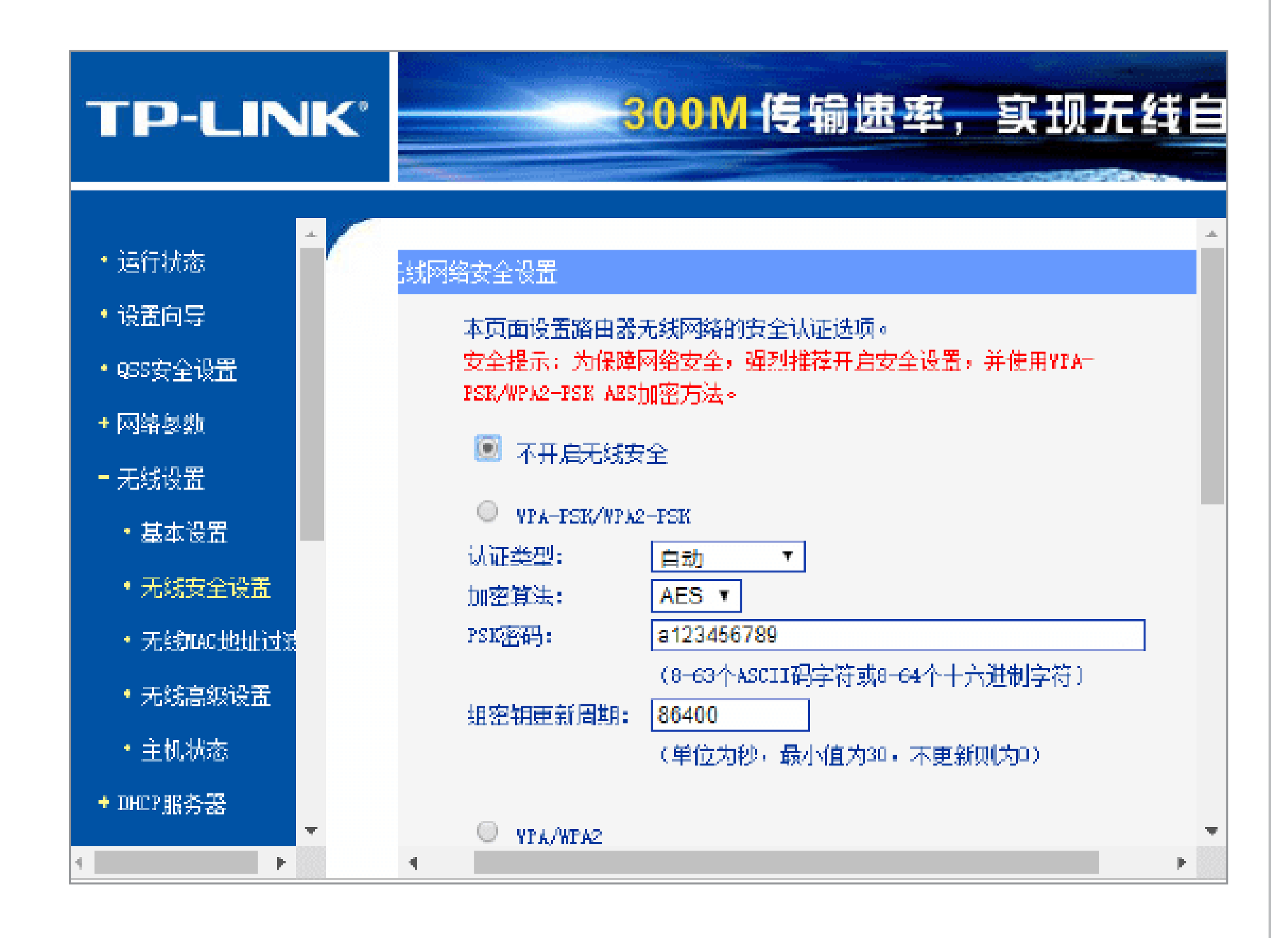


实战6：设置无线网络WPA-PSK密码

WPA-PSK可以看成是一个认证机制，只要求一个单一的密码进入每个无线局域网节点（如无线路由器），只要密码正确，就可以使用无线网络。下面介绍如何使用WPA-PSK或者WPA2-PSK加密无线网络。

1. 设置无线路由器WPA-PSK安全加密数据

Step 01 打开路由器的Web后台设置界面，选择“无线设置”→“无线安全设置”选项，进入“无线网络安全设置”界面，如下图所示。



Step 02 选中WPA-PSK/WAP2-PSK单选按钮，在“认证类型”下拉列表中选择“自动”选项，在“加密算法”下拉列表中选择“自动”选项，在“PSK密码”文本框中输入加密密码，本实例设置密码为sushi1986，单击“保存”按钮。



Step 03 单击“保存”按钮，弹出一个提示对话框，如下图所示，单击“确定”按钮，重新启动路由器即可。



2. 使用WPA-PSK安全加密认证的无线客户端

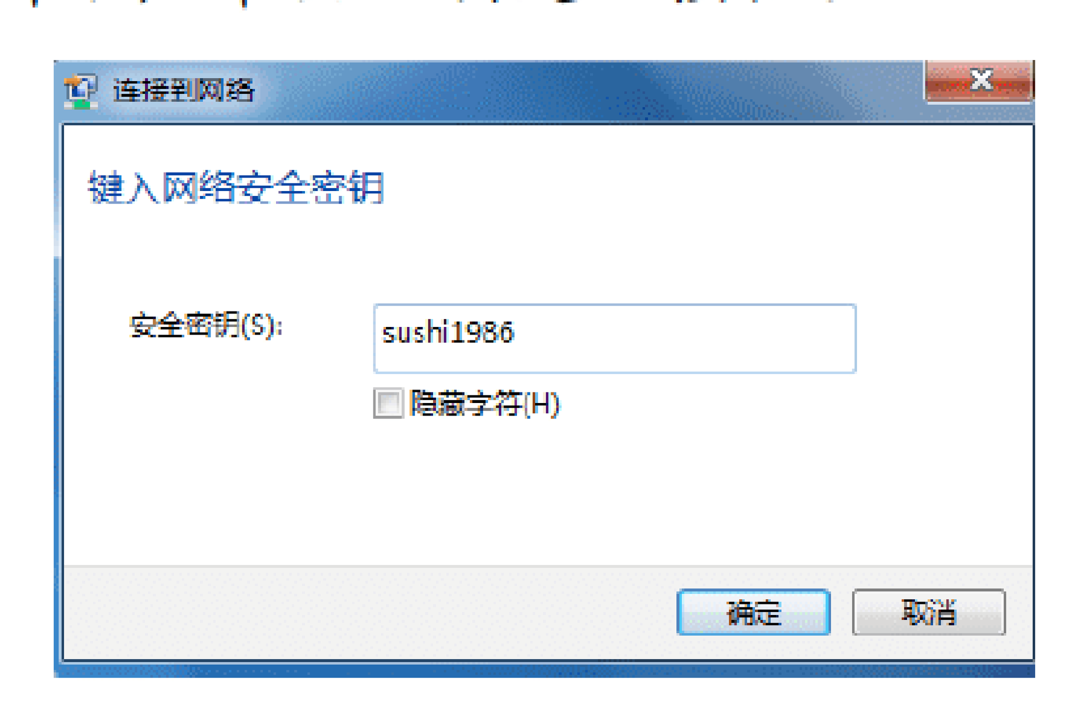
Step 01 单击系统桌面右下角“ ”图标，无线客户端会自动扫描区域内的无线信号，如下图所示。



Step 02 右击tp-link信号，在弹出的快捷菜单中选择“连接”选项，如下图所示。



Step 03 弹出“连接到网络”对话框，在“安全密钥”文本框中输入密码sushi1986，如下图所示，单击“确定”按钮。



Step 04 单击系统桌面右下角图标，将鼠标放在tp-link信号上，可以看到无线信号的连接情况，如下图所示，表明已经成功连接无线路由器。



提示：在WPA-PSK加密算法的使用过程中，密码设置应该尽可能复杂，并且要注意定期更改密码。

实战7：关闭路由器的SSID广播功能



SSID就是一个无线网络的名称，无线客户端通过无线网络的SSID来区分不同的无线网路。为了安全起见，往往要求无线AP关闭SSID广播，只有知道该无线网络SSID的人员才可以进行无线网络连接。

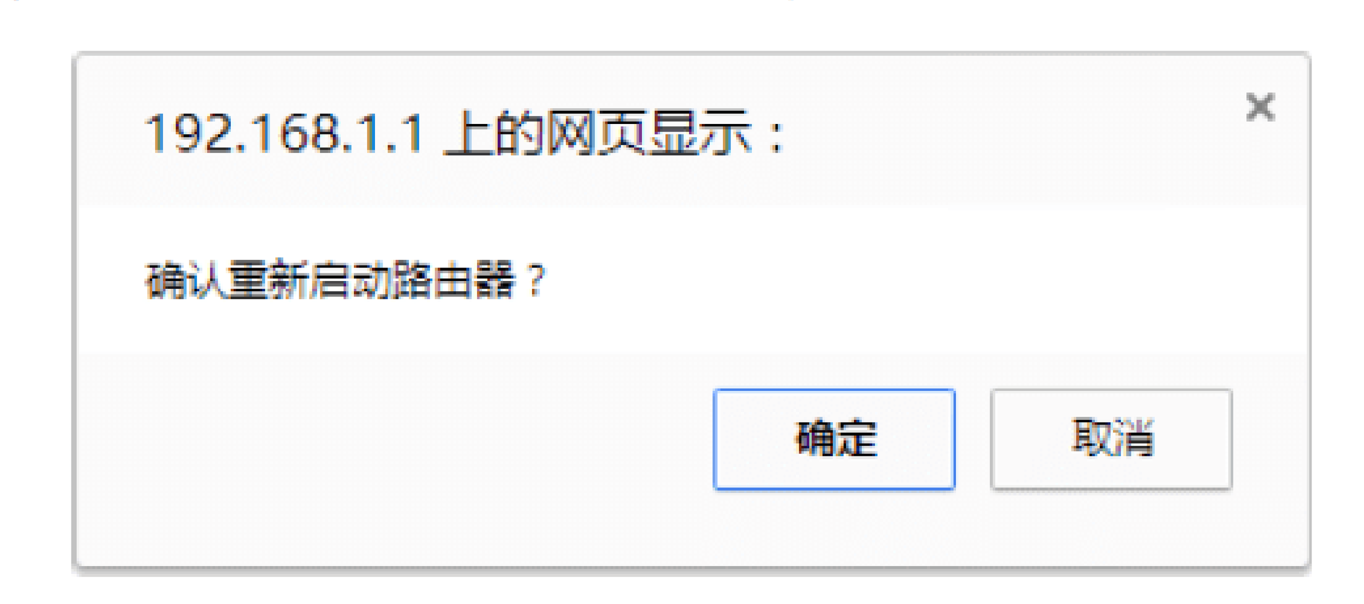
1. 关闭无线路由器的SSID广播

关闭无线路由器的SSID广播功能的具体操作步骤如下。

Step 01 打开路由器的Web后台设置界面，设置自己无线网络的SSID信息，取消勾选“允许SSID广播”复选框，如下图所示，单击“保存”按钮。



Step 02 弹出一个提示对话框，如下图所示，单击“确定”按钮，重新启动路由器。



2. 客户端连接

关闭SSID广播后，无线客户端连接的具体操作步骤如下。

Step 01 单击系统桌面右下角“ ”图标，会看到无线客户端自动扫描到区域内的所有无线信号，发现其中没有SSID为ssh的无线网络，但是会出现一个名称为“其他网络”的信号，如下图所示。



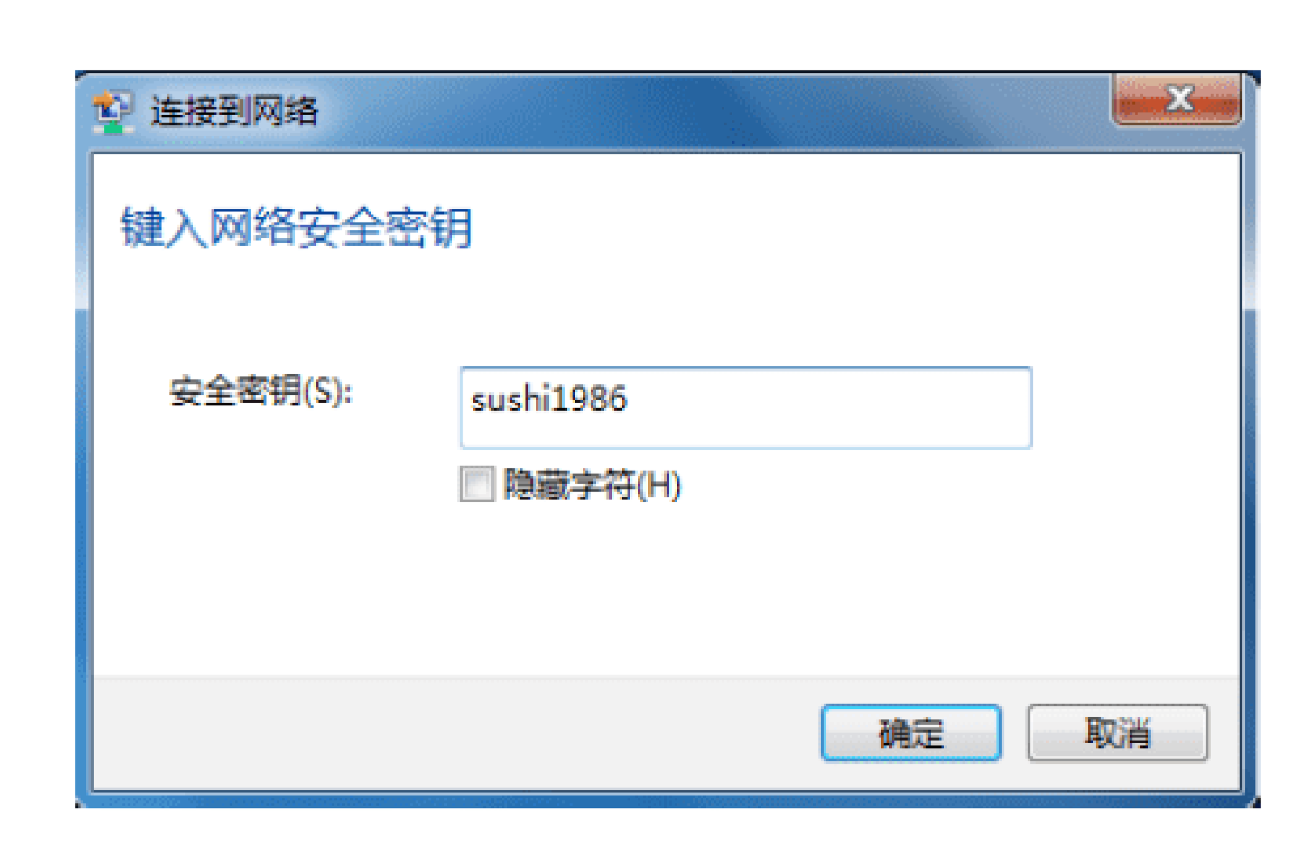
Step 02 右击“其他网络”，在弹出的快捷菜单中选择“连接”选项，如下图所示。



Step 03 弹出“连接到网络”对话框，在“名称”文本框中输入要连接网络的SSID号，本实例输入ssh，如下图所示，单击“确定”按钮。



Step 04 在“安全密钥”文本框中输入无线网络的密钥，本实例输入密钥为sushi1986，如下图所示，单击“确定”按钮。



Step 05 单击右下角“ ”图标，将鼠标放在ssh信号上，可以看到无线网络的连接情况，如下图所示，表明无线客户端已经成功连接到无线路由器。



实战8：使用无线网络开启MAC地址过滤功能

网络管理的主要任务之一就是控制客户端对网络的接入和对客户端的上网行为进行控制。无线网络也不例外，通常无线AP利用媒体访问控制（MAC）地址过滤的方法来限制无线客户端的接入。

使用无线路由器进行MAC地址过滤的具体操作步骤如下。

Step 01 打开路由器的Web后台设置界面，单击左侧“无线设置”→“MAC地址过滤”选项，默认情况MAC地址过滤功能是关闭状态，单击“启用过滤”按钮，开启MAC地址过滤功能，单击“添加新条目”按钮，如下图所示。

Step 02 打开“MAC地址过滤”对话框，在“MAC地址”文本框中输入无线客户端的MAC地址，本实例输入MAC地址为00-0C-29-5A-3C-97，在“描述”文本框中输入MAC描述信息sushipc，在“类型”下拉列表中选择“允许”选项，在“状态”下拉列表中选择“生效”选项，如下图所示。依照此步骤将所有合法的无线客户端的MAC地址加入到此MAC地址表，单击“保存”按钮。

Step 03 选中“过滤规则”选项下的“禁止”单选按钮，表明在下面MAC列表中生效规则之外的MAC地址不可以访问无线网络，如下图所示。

Step 04 这样无线客户端在访问无线AP时，会发现除了MAC地址表中的MAC地址之外，其他的MAC地址无法再访问无线AP，也就无法访问互联网。

10.4 无线路由器的安全防护

使用无线路由管理工具可以方便管理无线网络中的上网设备，本节介绍两个无线路由安全管理工具，包括《360路由器卫士》与《路由优化大师》。

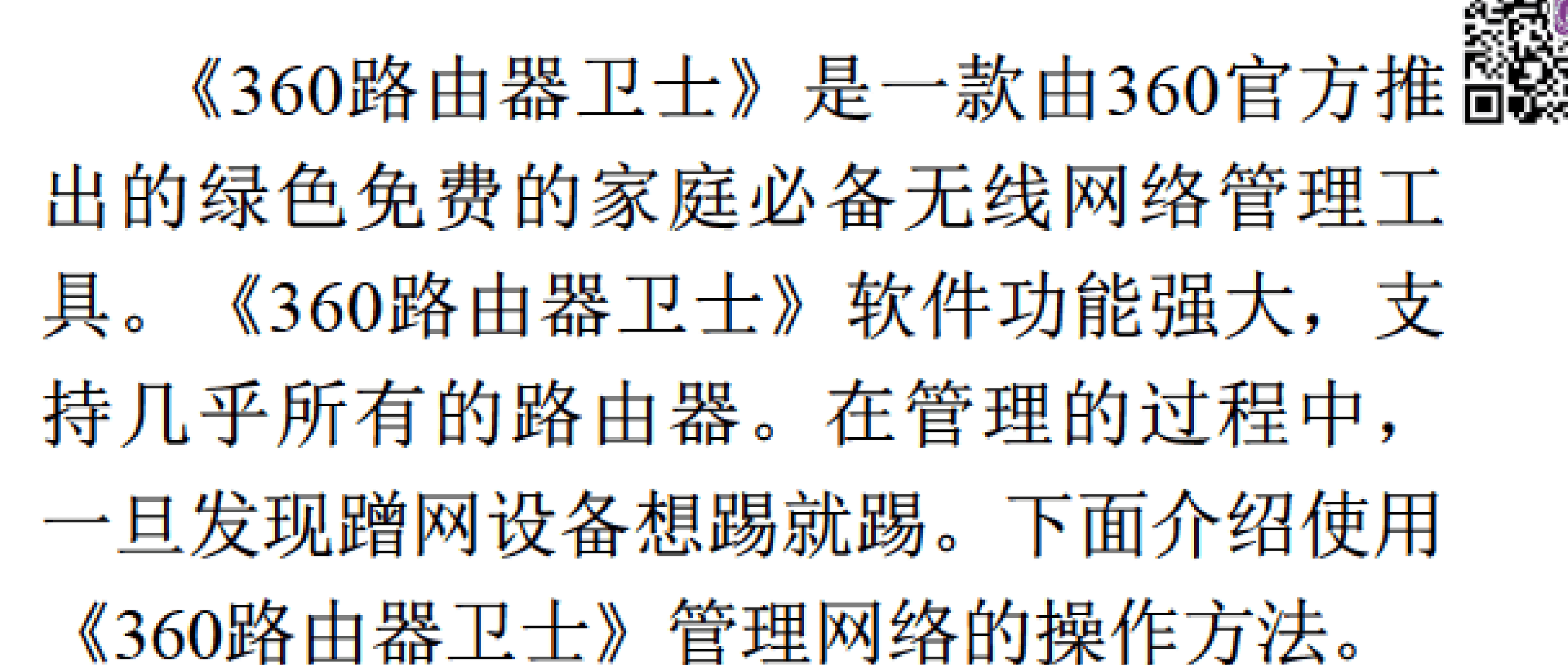
实战9：使用《360路由器卫士》防护

《360路由器卫士》是一款由360官方推出的绿色免费的家庭必备无线网络管理工具。《360路由器卫士》软件功能强大，支持几乎所有的路由器。在管理的过程中，一旦发现蹭网设备想踢就踢。下面介绍使用《360路由器卫士》管理网络的操作方法。

Step 01 下载并安装360路由器卫士，双击桌面上的快捷图标，打开“路由器卫士”工作界面，提示用户正在连接路由器，如下图所示。



Step 02 连接成功后，在弹出对话框中分别输入路由器的账号与密码，如下图所示。



Step 03 单击“下一步”按钮，进入“我的路由”工作界面，在其中可以看到当前的在线设备，如下图所示。



Step 04 如果想要对某个设备限速，则可以单击设备后的“限速”按钮，打开“限速”对话框，在其中设置设备的上传速度与下载速度，如下图所示，设置完毕，单击“确认”按钮即可保存设置。



Step 05 在管理的过程中，一旦发现有蹭网设备，可以单击该设备后的“禁止上网”按钮，如下图所示。



Step 06 禁止上网后，单击“黑名单”选项卡，进入“黑名单”设置界面，在其中可以看到被禁止的上网设备，如下图所示。



Step 07 选择“路由防黑”选项卡，进入“路由防黑”设置界面，在其中可以对路由器进行防黑检测，如下图所示。



Step 08 单击“立即检测”按钮，即可开始对路由器进行检测，并给出检测结果，如下图所示。



Step 09 选择“路由跑分”选项卡，进入“路由跑分”设置界面，在其中可以查看当前路由器信息，如下图所示。



Step 10 单击“开始跑分”按钮，即可开始评估当前路由器的性能，如下图所示。



Step 11 评估完成后，会在“路由跑分”界面中给出跑分排行榜信息，如下图所示。

Step 12 选择“路由设置”选项卡，进入“路由设置”设置界面，如下图所示，在其中可以对宽带上网、WiFi密码、路由器密码等选项进行设置。

Step 13 选择“路由时光机”选项，在打开的界面中单击“立即开启”按钮，即可打开“时光机开启”设置界面，如下图所示，在其中输入360账号与密码，然后单击“立即登录并开启”按钮，即可开启时光机。

Step 14 选择“宽带上网”选项，进入“宽带上网”界面，如下图所示，在其中输入网络运营商给出的上网账号与密码，单击“保存设置”按钮，即可保存设置。



Step 15 选择“WiFi密码”选项，进入“WiFi密码”界面，如下图所示，在其中输入WiFi密码，单击“保存设置”按钮，即可保存设置。



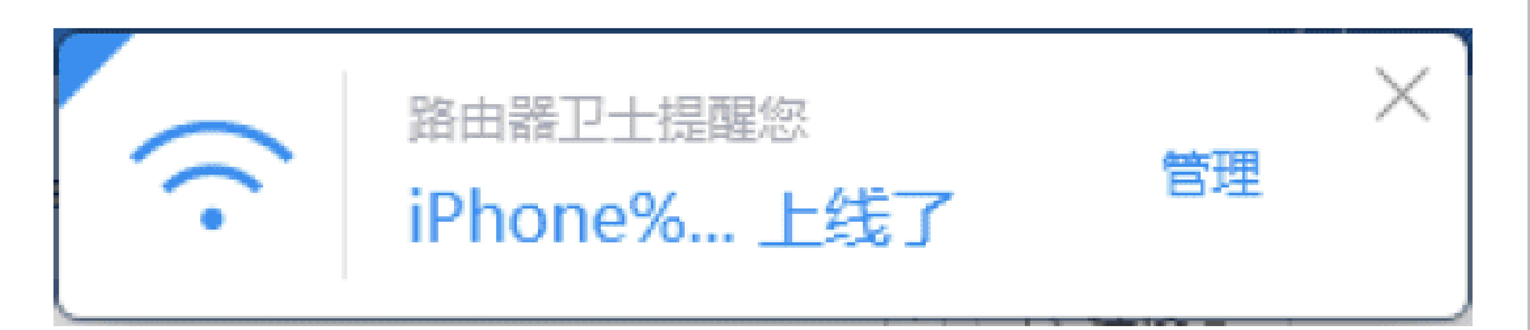
Step 16 选择“路由器密码”选项，进入“路由器密码”界面，如下图所示，在其中输入路由器密码，单击“保存设置”按钮，即可保存设置。



Step 17 选择“重启路由器”选项，进入“重启路由器”界面，如下图所示，单击“重启”按钮，即可对当前路由器进行重启操作。



另外，使用360路由器卫士在管理无线网络安全的过程中，一旦检测到有设备通过路由器上网，就会在计算机桌面的右上角弹出信息提示框，如下图所示。



单击“管理”按钮，即可打开该设备的详细信息界面，如下图所示，在其中可以对网速进行限制管理，最后单击“确认”按钮即可。



实战10：使用《路由优化大师》防护

《路由优化大师》是一款专业的路由器设置软件，其主要功能有一键设置优化路由、屏广告、防蹭网、路由器全面检测及高级设置等，从而保护路由器安全。

使用《路由优化大师》管理无线网络安全的操作步骤如下。

Step 01 下载并安装路由优化大师，双击桌面上的快捷图标，即可打开“路由优化大师”的工作界面，如下图所示。



Step 02 单击“登录”按钮，打开RMTools窗口，在其中输入管理员密码，如下图所示。



Step 03 单击“确定”按钮，即可进入路由器工作界面，在其中可以看到主人网络和访客网络信息，如下图所示。



Step 04 单击“设备管理”图标，进入“设备管理”工作界面，在其中可以看到当前无线网络中的连接设备，如下图所示。



Step 05 如果想要对某个设备进行管理，则可以单击“管理”按钮，进入该设备的管理界面，在其中可以设置设备的上传速度、下载速度以及上网时间等信息，如下图所示。



Step 06 单击“添加允许上网时间段”超链接，即可打开上网时间段的设置界面，在其中可以设置时间段描述信息、开始时间、结束时间等，如下图所示。



Step 07 单击“确定”按钮，即可完成上网时间段的设置操作，如下图所示。



Step 08 单击“应用管理”图标，即可进入“应用管理”工作界面，在其中可以看到路由优化大师为用户提供的应用程序，如下图所示。



Step 09 如果想要使用某个应用程序，则可以单击某应用程序下的“进入”按钮，进入该应用程序的设置界面，如下图所示。



Step 10 单击“路由设置”图标，在打开的界面中可以查看当前路由器的设置信息，如下图所示。

Step 11 选择左侧的“上网设置”选项，在打

开的界面中可以对当前的上网信息进行设置，如下图所示。

基本设置
上网方式 宽带拨号上网
宽带帐号 18099921808
宽带密码 ••••••
IP地址 49.117.106.249
DNS服务器 61.128.114.134 , 61.128.114.167
在线时长 2天9小时59分钟
断开 连接

Step 12 选择“无线设置”选项，在打开的界面中可以对路由的无线功能进行开关、名称、密码等信息设置，如下图所示。

无线设置
无线功能 开 关
无线名称 千谷科技 开启无线广播
无线密码 feiyu123456
无线信道 自动
无线模式 11bgn mixed
频段带宽 自动
保存

Step 13 选择“LAN口设置”选项，在打开的界面中可以对路由的LAN口IP进行设置，如下图所示。

LAN口设置
MAC地址 F4-83-CD-33-60-73
LAN口IP设置 自动（推荐）
IP地址 192.168.0.1
子网掩码 255.255.255.0
保存

Step 14 选择“DHCP服务器”选项，在打开的界面中可以对路由的DHCP服务器进行设置，如下图所示。



Step 15 选择“在线升级”选项，在打开的界面中可以对路由优化大师的版本进行升级操作，如下图所示。



Step 16 选择“修改管理员密码”选项，在打开的界面中可以对管理员密码进行修改设置，如下图所示。



Step 17 选择“备份和载入配置”选项，在打开的界面中可以对当前路由器的配置进行备份和载入设置，如下图所示。



Step 18 选择“重启和恢复出厂”选项，在打开的界面中可以对当前路由器进行重启和恢复出厂设置，如下图所示。



Step 19 选择“系统日志”选项，在打开的界面中可以查看当前路由器的系统日志，如下图所示。

系统日志

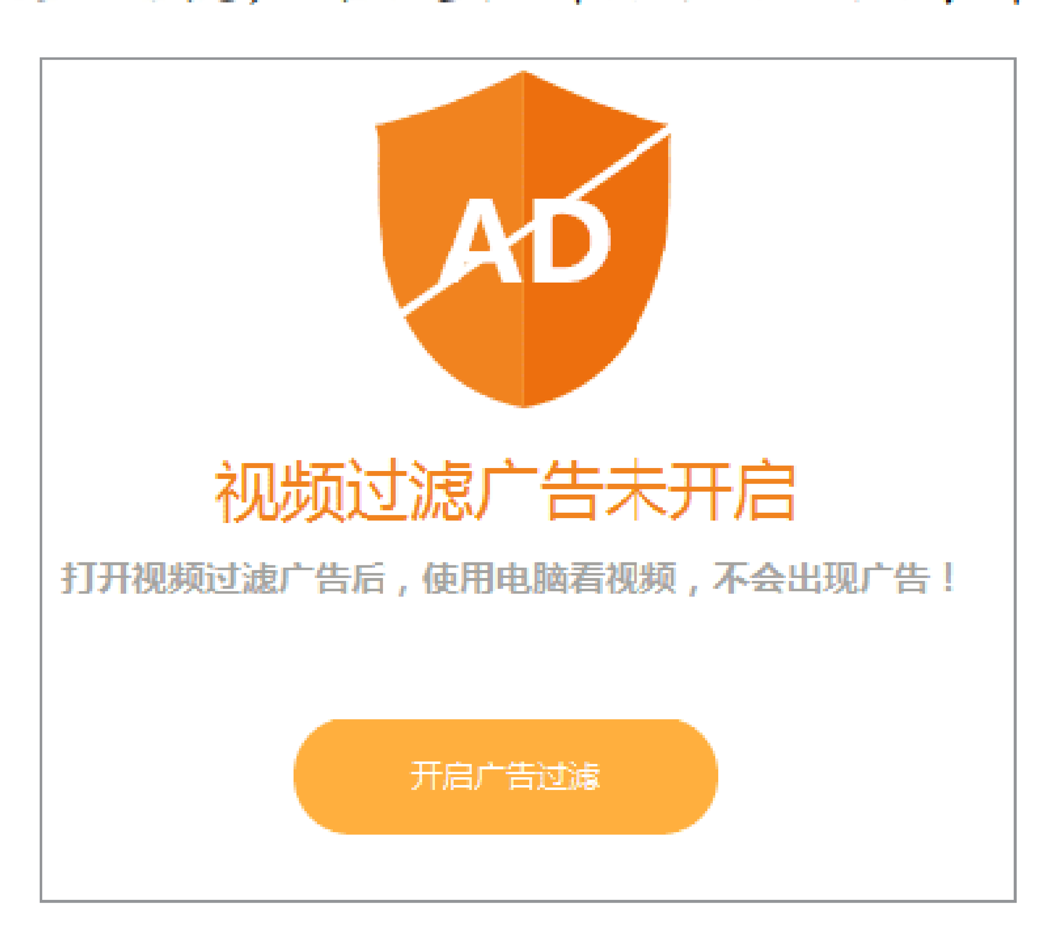
刷 新　保存所有日志　清除所有日志

索引	类型	日志内容
140	ERR	16days, 09:39:23,"wlan2" is not attached to MUX.
139	INFO	16days, 09:00:57,DHCPS: Send OFFER with ip 192.168.0.102.
138	INFO	16days, 08:54:33,DHCPS: Send OFFER with ip 192.168.0.102.
137	INFO	16days, 08:29:41,DHCPS: Send OFFER with ip 192.168.0.114.
136	INFO	16days, 07:12:45,DHCPS: Send OFFER with ip 192.168.0.105.
135	INFO	16days, 07:12:37,DHCPS: Send OFFER with ip 192.168.0.108.
134	INFO	16days, 07:12:33,DHCPS: Send OFFER with ip 192.168.0.103.
133	INFO	16days, 07:12:10,DHCPS: Send OFFER with ip 192.168.0.102.

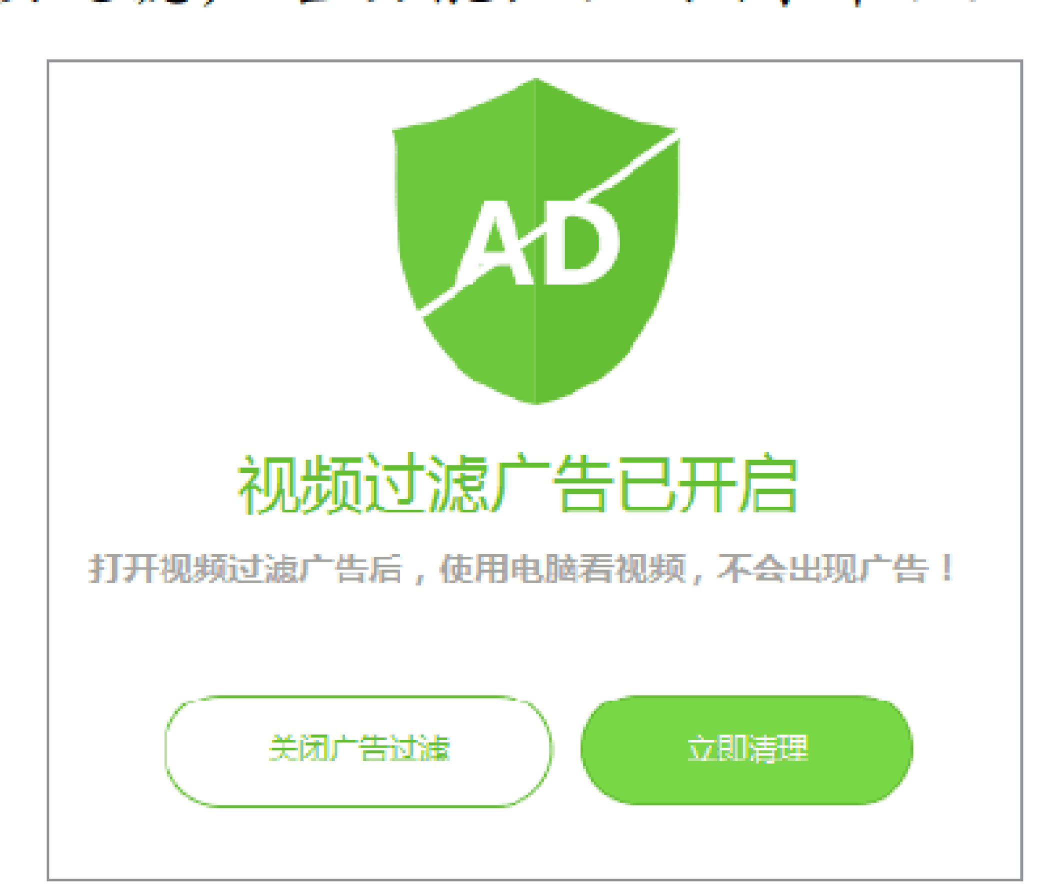
Step 20 路由器设备设置完毕后，返回到“路由优化大师”的工作界面中，选择“防蹭网”选项，在打开的界面中可以进行防蹭网设置，如下图所示。



Step 21 选择“屏广告”选项，在打开的界面中可以设置过滤广告是否开启，如下图所示。



Step 22 单击“开启广告过滤”按钮，即可开启视频过滤广告功能，如下图所示。



Step 23 单击“立即清理”按钮，即可清理广告信息，如下图所示。



Step 24 选择“测网速”选项，进入“网速测试”设置界面，如下图所示。



Step 25 单击“开启测速”按钮，即可对当前网络进行测速操作，测出来的结果显示在工作界面中，如下图所示。





10.5 实战演练



实战演练1——控制无线网中设备的上网速度

在无线局域网中所有的终端设备都是通过路由器上网的，为了更好地管理各个终端设备的上网情况，管理员可以通过路由器控制上网设备的上网速度，具体的操作步骤如下。

Step 01 打开路由器的Web后台设置界面，在其中选择“IP宽带控制”选项，在右侧的窗格中可以查看相关的功能信息，如下图所示。



Step 02 勾选“开启IP宽带控制”复选框，即可在下方的设置区域中对设备的上行总带宽和下行总带宽进行设置，进而控制终端设置的上网速度，如下图所示。



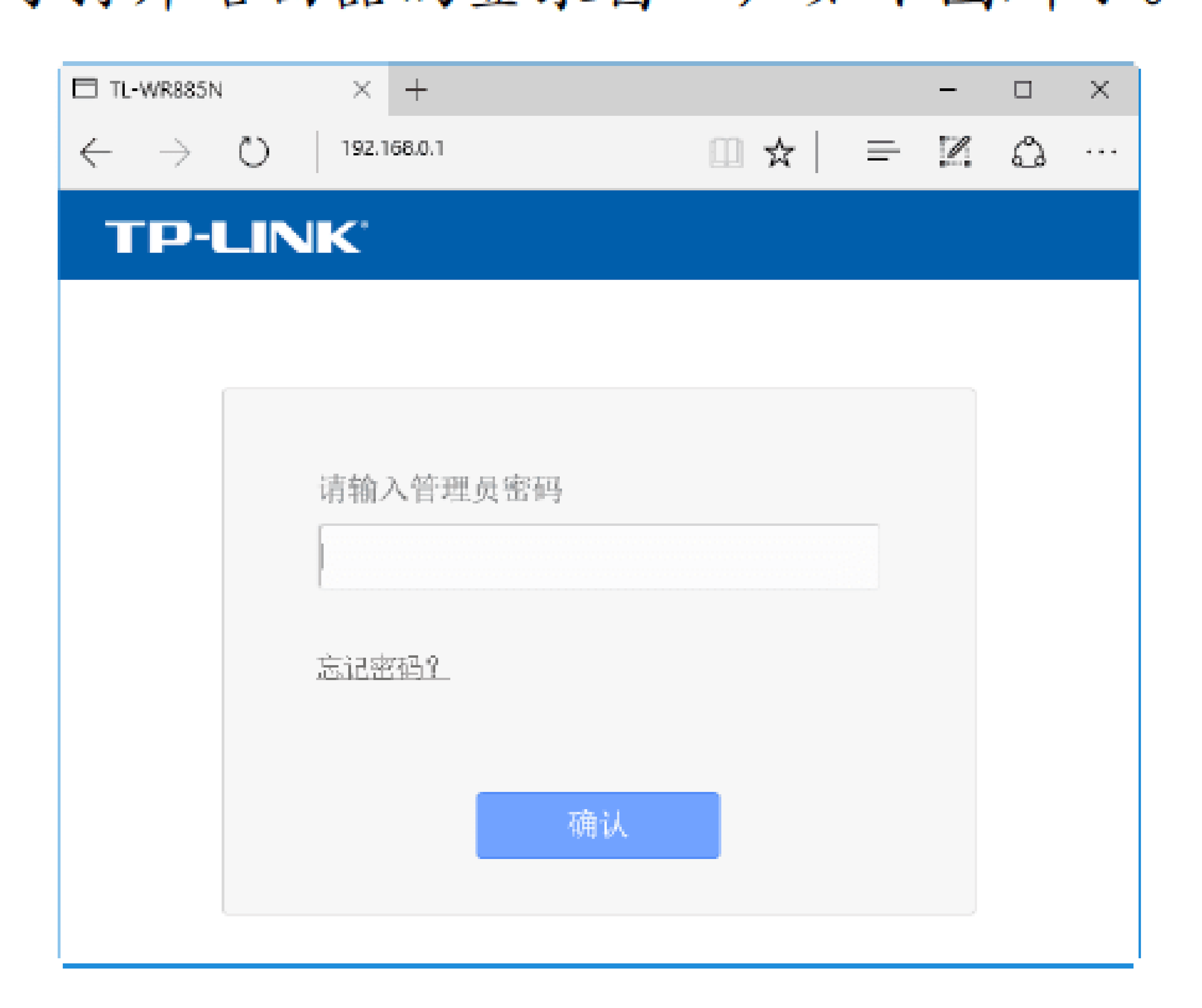
实战演练2——通过向导设置路由器并进行上网

目前多数家用型无线路由器都提供了网页进入页面，当用户登录路由器后会提供一个向导，通过向导设置可以最快地实现连接外网。家用路由器背面会有路由器型号、路由器IP（进入路由器的地址）、管理员账号密码等信息，如下图所示。



通过向导设置路由器并进行上网的具体操作步骤如下。

Step 01 打开IE浏览器，在地址栏中输入路由器的网址，一般情况下路由器的默认网址为192.168.0.1，输入完毕后单击“转至”按钮，即可打开路由器的登录窗口，如下图所示。



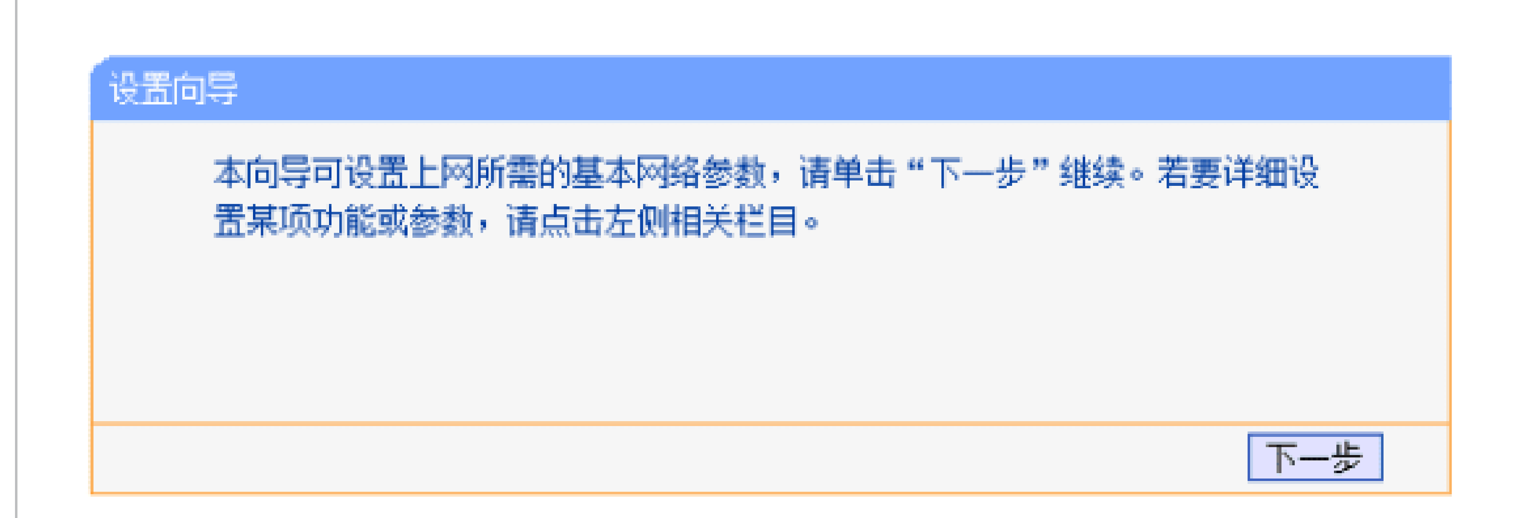
Step 02 在“请输入管理员密码”文本框中输入管理员的密码，默认情况下管理员的密码为“123456”，如下图所示。



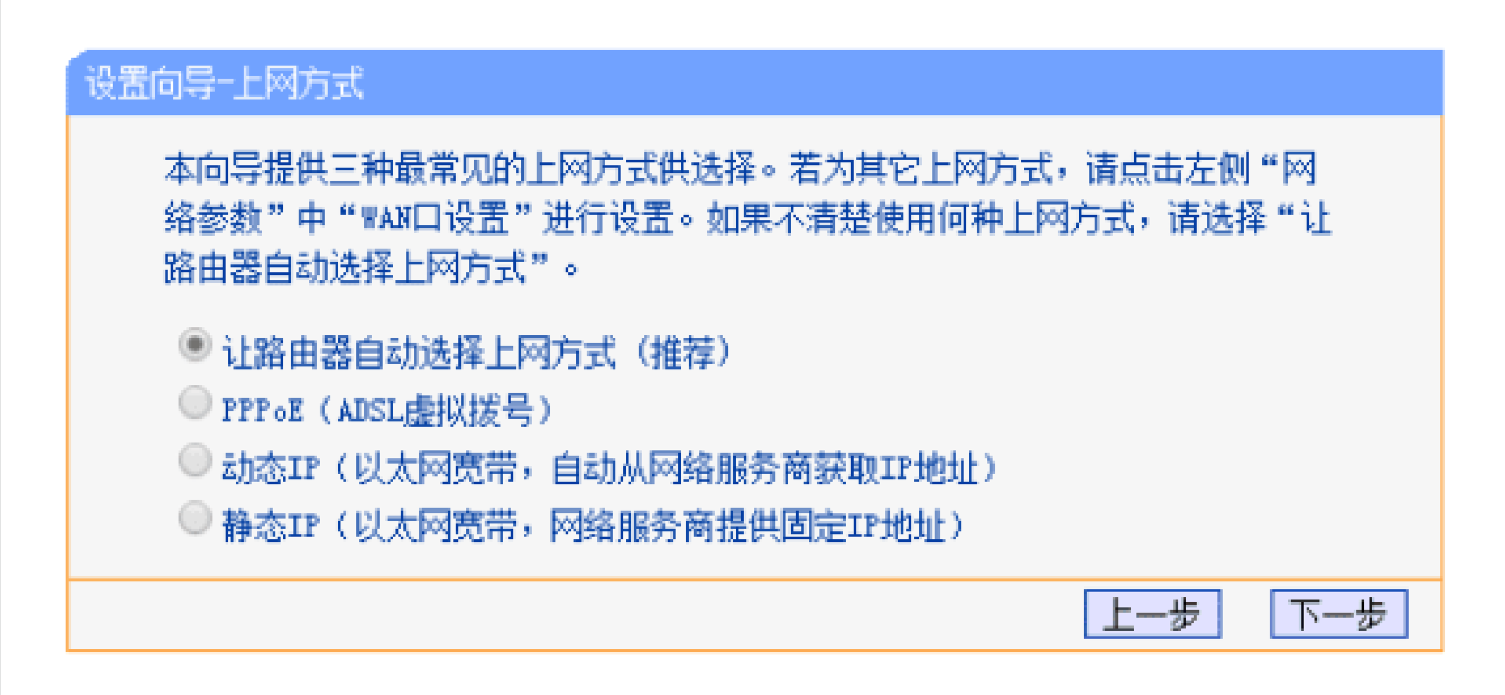
Step 03 单击“确认”按钮，即可进入路由器的“运行状态”工作界面，在其中可以查看路由器的基本信息，如下图所示。



Step 04 选择“设置向导”选项，即可进入“设置向导”页面，如下图所示。



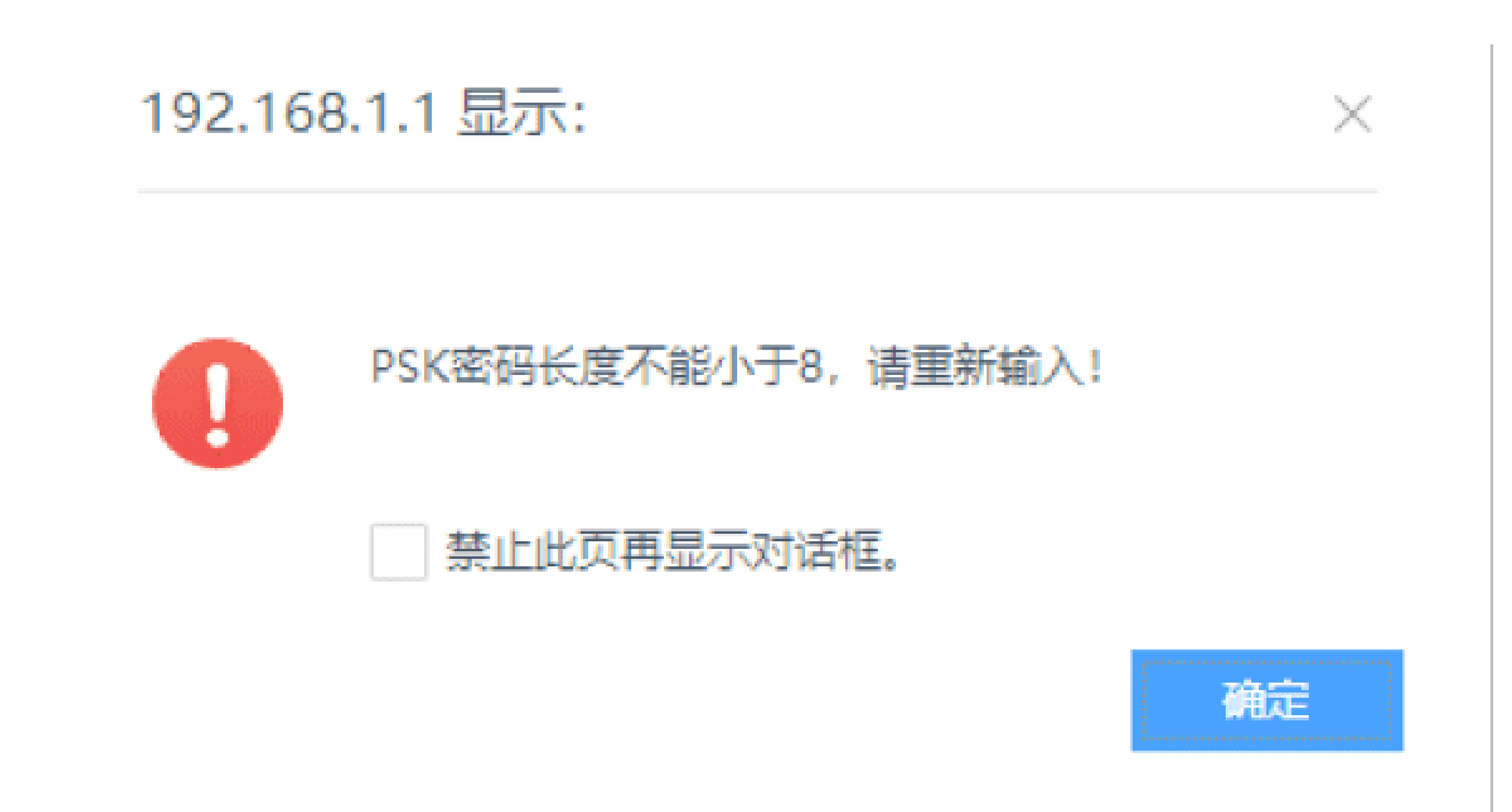
Step 05 单击“下一步”按钮，进入“设置向导-上网方式”界面，在其中选择上网方式，其中PPPoE为拨号上网，一般由运营商提供具体账号密码，动态IP和静态IP则多为分网时使用，可以根据实际需求选择，如下图所示。



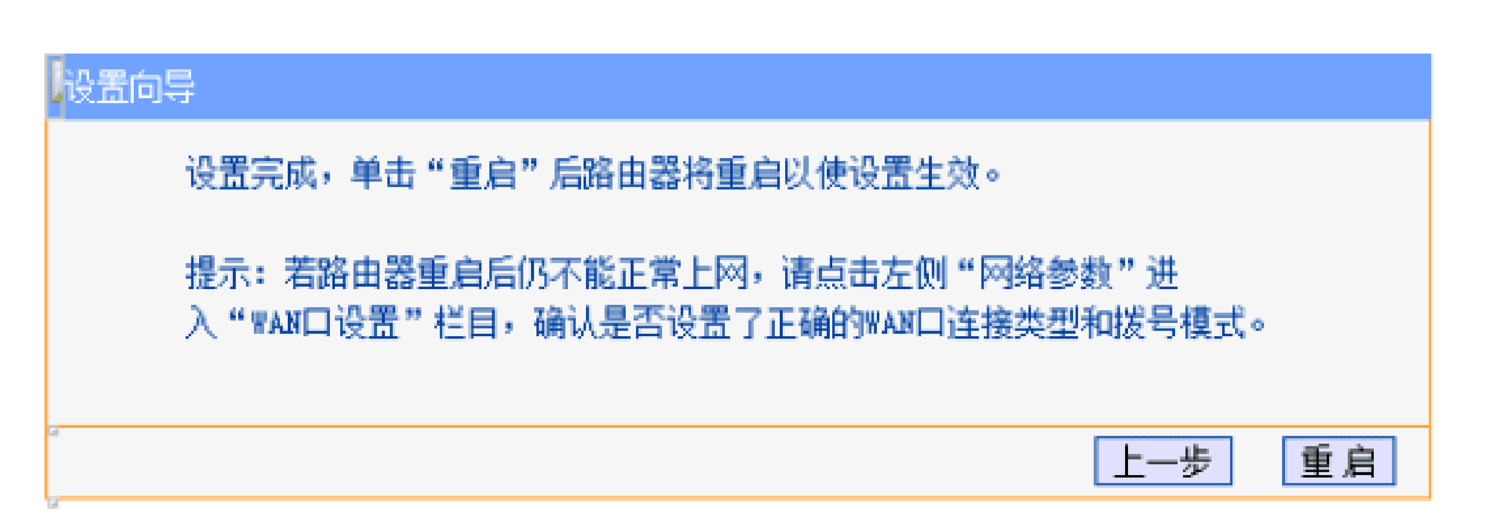
Step 06 单击“下一步”按钮，进入“设置向导-无线设置”界面，在其中设置路由器无线网络的基本参数以及无线安全，安全选项可以采用WPA-PSK/WPA2-PSK这种方式输入密码，如下图所示。

设置向导 － 无线设置
本向导页面设置路由器无线网络的基本参数以及无线安全。
无线状态：开启
SSID：TP-LINK_012F08
信道：自动
模式：11bgn mixed
频段带宽：自动
无线安全选项：
为保障网络安全，强烈推荐开启无线安全，并使用WPA-PSK/WPA2-PSK AES加密方式。
不开启无线安全
WPA-PSK/WPA2-PSK
PSK密码：
（8-63个ASCII码字符或8-64个十六进制字符）
不修改无线安全设置
上一步　下一步

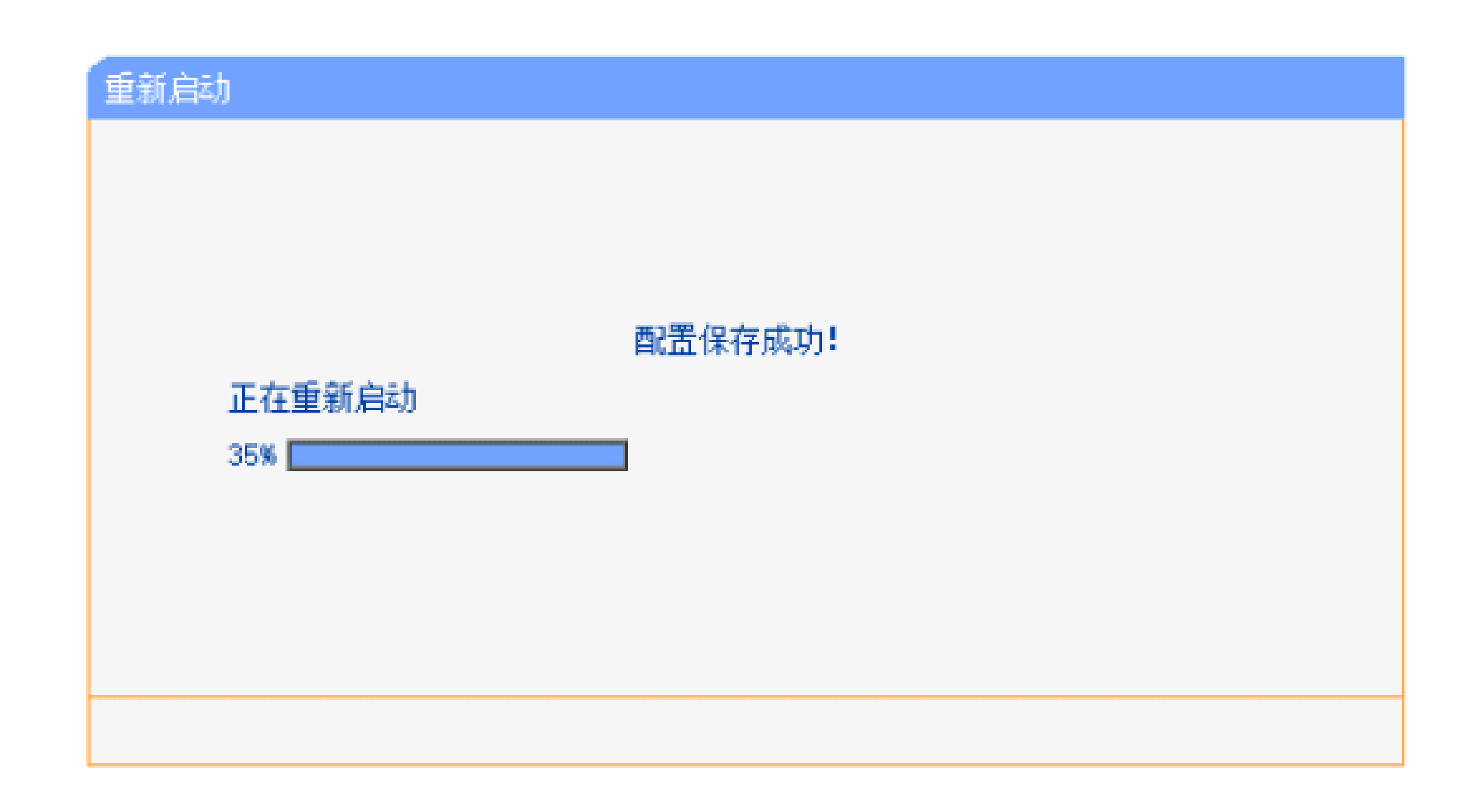
注意：无线密码不能小于8，否则会有提示，如下图所示。



Step 07 单击“下一步”按钮，即可完成向导设置，并弹出如下图所示的界面。



Step 08 单击“重启”按钮，重启路由器，如下图所示，等待路由器重启完成后，就可以进行上网了。



10.6 小试身手



练习1：加密手机的WLAN热点功能

为保证手机的安全，一般需要给手机的WLAN热点功能添加密码，具体的操作步骤如下。

Step 01 在手机的移动热点设置界面中，点按“配置WLAN热点”功能，在弹出的界面中点按“开放”选项，可以选择手机设备的加密方式，如下图所示。



Step 02 选择好加密方式后，即可在下方显示密码输入框，在其中输入密码，如下图所示，然后单击“保存”按钮即可。



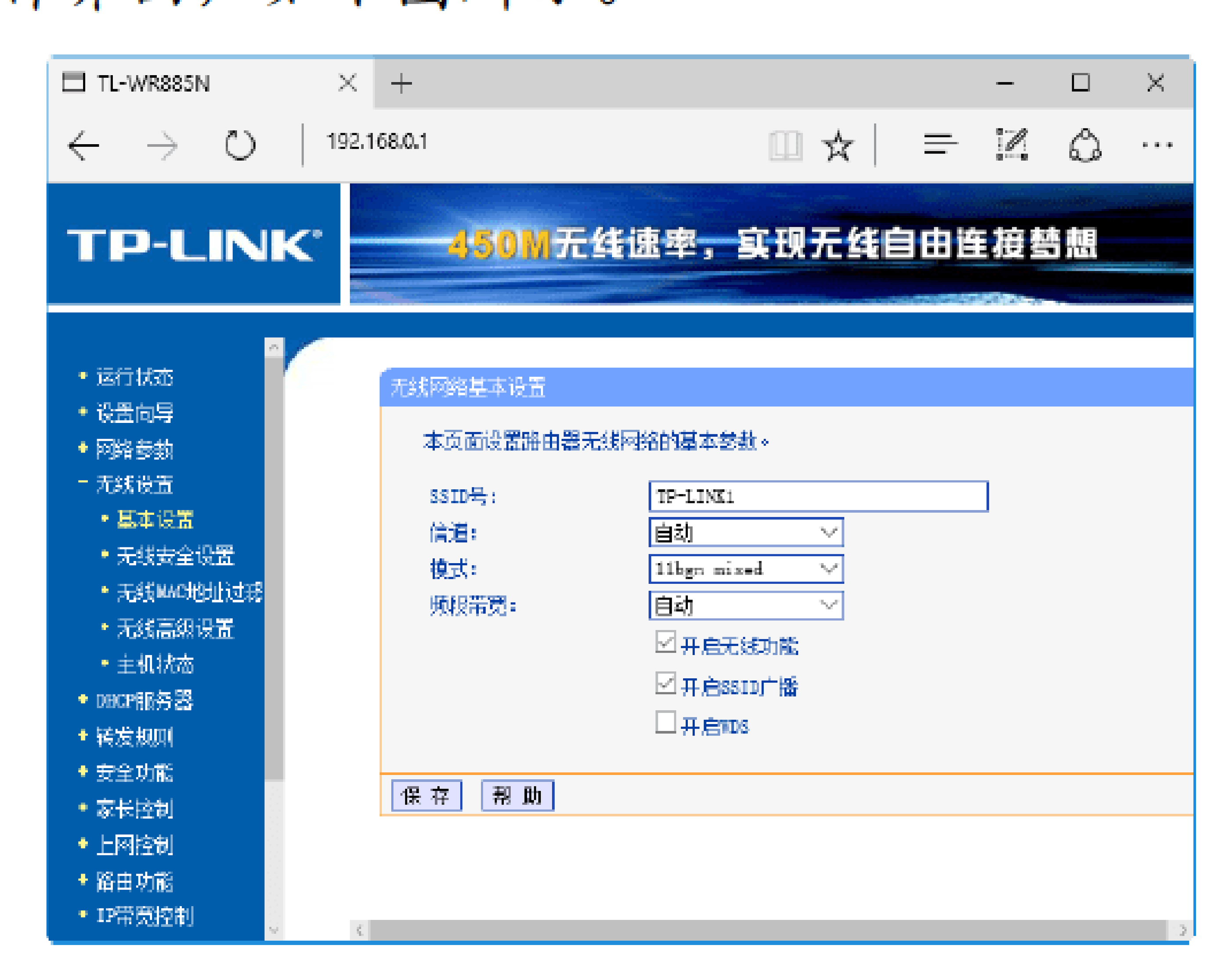
Step 03 加密完成后，使用计算机再连接手机设备时，系统提示用户输入网络安全密钥，如下图所示。



练习2：通过修改WiFi名称隐藏路由器

WiFi的名称通常是指路由器当中SSID号的名称，该名称可以根据自己的需要进行修改，具体的操作步骤如下。

Step 01 打开路由器的Web后台设置界面，在其中选择“无线设置”选项下的“基本设置”选项，打开“无线网络基本设置”工作界面，如下图所示。



Step 02 将SSID号的名称由TP-LINK1修改为wifi，如下图所示，单击“确定”按钮，即可保存WiFi修改后的名称。





第11章 网站系统的安全防护

网站攻击技术无处不在，在某个安全程序非常高的网站，攻击者也许只用小小的一句代码就可以让网站成为入侵者的帮凶，让网站访问者成了最无辜的受害者。本章介绍网站系统的安全防护实战，主要内容包括网站基础知识、DoS攻击、DDoS攻击、SQL注入攻击和网站攻击的安全防护方法等。

11.1 认识网站和网页

在创建网站之前，首先需要认识什么是网页、什么是网站以及网站的种类与特点。本节介绍一下它们的相关概念。

11.1.1 什么是网站

网站就是在因特网上通过超链接的形式构成的相关网页的集合。简单地说，网站是一种通信工具，人们可以通过网页浏览器来访问网站，获取自己需要的资源或享受网络提供的服务。例如，人们可以通过网上菜市场网站查找自己需要的果蔬信息，如下图所示。



11.1.2 网站的分类

按照内容和形式的不同，网站可以分为门户网站、职能网站、专业网站和个人网站四大类。

1. 门户网站

门户网站是指涉及领域非常广泛的综合性网站，如国内著名的三大门户网站：网易、搜狐和新浪。下图为网易网站的首页。



2. 职能网站

职能网站是指一些公司为展示其产品或对其所提供的售后服务进行说明而建立的网站。下图为联想集团的中文官方网站。



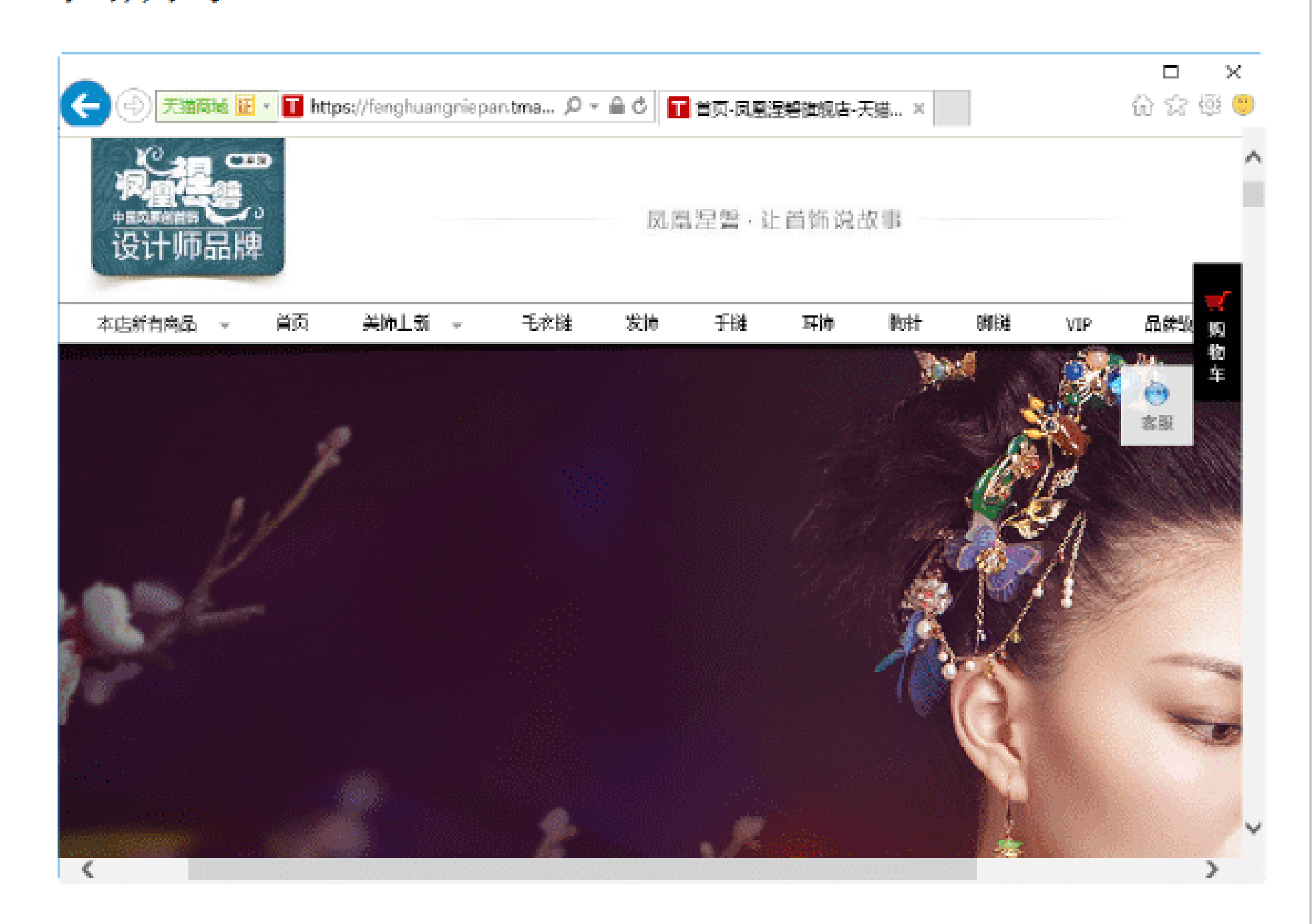
3. 专业网站

专业网站是指专门以某个主题为内容而建立的网站，这种网站都是以某一题材的信息作为网站的内容的。下图为赶集网网站，该网站主要为用户提供租房、二手货交易等同城相关服务。



4. 个人网站

个人网站是指由个人开发建立的网站，在内容形式上具有很强的个性化，通常用来宣传自己或展示个人的兴趣爱好。例如淘宝网，在淘宝网上注册一个账户，开一家自己的小店，在一定程度上既宣传了自己，又展示了个人兴趣与爱好，如下图所示。



11.1.3　什么是网页

网页是因特网中最基本的信息单位，是把文字、图形、声音及动画等各种多媒体信息相互链接起来而构成的一种信息表达方式。通常，网页中有文字和图像等基本信息，有些网页中还有声音、动画和视频等多媒体内容。

在访问一个网站时，首先看到的网页一般称为该网站的首页。有些网站的首页只是网站的开场页，具有欢迎访问者的作用，单击页面上的文字或图片，可打开网站的主页，而首页也随之关闭，如下图所示。



网站的主页与首页的区别在于：主页设有网站的导航栏，是所有网页的链接中心。但多数网站的首页与主页通常合为一个页面，即省略了首页直接显示主页。在这种情况下，它们指的是同一个页面，如下图所示。



在攻击网站之前，用户还需要认识网页有哪些组成部分。通常，网页包括网址、网页标题、LOGO、文本、导航栏、超链接、图像、表单、动画、按钮等内容。

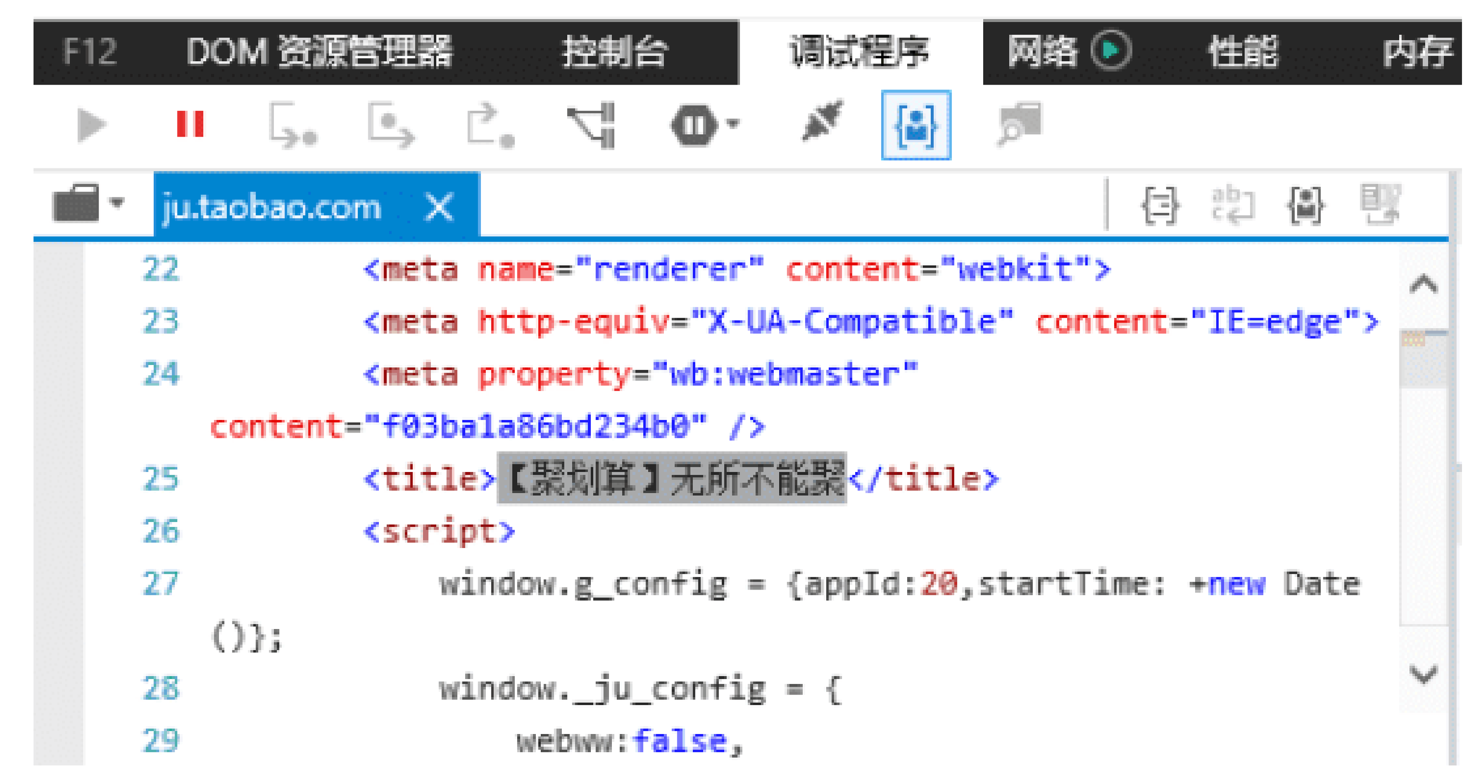
（1）网址是指互联网上网页的地址。每个网页都有唯一的网址，在浏览器的地址栏中输入该网址即可浏览该网址对应的网页，如下图为通过网址访问百度。



（2）网页标题是对一个网页的高度概括，通常而言，网站首页的标题就是网站的正式名称，如下图所示。



在网页中的HTML代码中，网页标题位于<head></head>标签之间的<title>标签之中，如下图所示。




```
<meta name="renderer" content="webkit">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta property="wb:webmaster"
content="f03ba1a86bd234b0" />
<title>【聚划算】无所不能聚</title>
<script>
    window.g_config = {appId:20,startTime: +new Date
()};
    window._ju_config = {
        webww:false,
```

（3）网络中的LOGO是网站的标志，主要用于与其他网站交换链接，在设计和制作的网页中，LOGO通常用图像和动画制作，如下图为携程网的LOGO标志。



（4）在网页中，文本内容是网页中信息传递的主要载体，是非常重要的网页元素，如下图所示。



（5）图像是网页中的主要元素之一，通过图像，不仅可以美化网页的外观，还可以让浏览者更直观地了解信息，如下图所示。



（6）导航栏是一系列的导航按钮，其作用是链接到各个页面，让浏览者可以快速找到需要的资源，导航栏一般位于网页的顶端或左侧，如下图所示。



另外，导航栏中只有水平导航栏和垂直导航栏两种，要制作导航栏，用户可以使用文本、图像、按钮、动画等网页元素来实现，如下图为网页中的垂直导航栏。



（7）超链接是网页中的一个重要组成部分，通过它可以快速跳转到当前网站的另一个页面，或者另一个网站的某个页面，只有通过超链接将各个页面组织在一起，才能真正构成一个网站。在网页中，将鼠标指针移动到对象上，其变为手的形状，说明该对象是超链接，如下图所示。



（8）在网页中，表单主要用于数据采集，如收集用户填写的注册资料、搜集用户的反馈信息、获取用户登录的用户名和密码等，如下图所示。



（9）网页中的动画可以是GIF格式的，还可以是Flash动画，尤其是Flash动画，由于其占用的存储空间很小，而且可以与动态网页和数据库进行信息交互，因此，非常适合在网页中使用，如下图为网页中的动画。



（10）Banner是网页中的一种元素，它可以作为网站页面的横幅广告或者宣传网页内容等。在网页设计中，该部分是嵌入在页面中的，通过图像或者动画制作，如下图为苏宁易购中的Banner广告。



11.2　网站攻击基础知识

在学习网站攻防知识前，用户需要了解网站攻击的原理与特点。

11.2.1　网站攻击的原理

网站攻击的手段多种多样，其基本原理是：网站攻击者利用网站服务器操作系统自身存在的或因配置不当而产生的安全漏洞、网站编写所使用语言程序本身所具有的安全隐患等，通过网站攻击命令、从网上下载的专用软件或自己编写的攻击软件非法进入网站服务器系统，从而获得网站服务器的管理权限，进而非法修改、删除网站系统中的重要信息或在网站服务器的系统中添加垃圾、色情和有害信息（如特洛伊木马）等。



11.2.2　网站攻击的特点

网站攻击的主要特点包括以下几个方面：

（1）广泛性。目前，由于网络上各种各样的网站数不胜数，因此给网站攻击者提供了众多的攻击目标。可以说，有网站的地方就有网站攻击的存在，应用比较广泛。

（2）多样性。网站攻击的手段多种多样，主要是因为网站服务器各不相同，且使用的网站编程程序也不尽相同，不同的网站服务器和网站程序都有可能存在着不同的漏洞，因此使得网站的攻击手段极为多样。

（3）危害性。网站攻击的危害性极大，轻者导致网站服务器无法正常运行，重者可以盗取网站用户中的重要信息，造成整个网站的瘫痪，甚至还可以控制整个网站服务器。

（4）难于防范性。对于网站的攻击很难防范，因为每个网站所采用的网站编程程序不尽相同，所产生的漏洞也不相同，很难采用统一的方式为漏洞打补丁。另外，网站的攻击不会在防火墙或系统日志中留下任何入侵痕迹，致使网络管理员也很难从网站日志里查找到入侵者的足迹。

11.3　网站攻击的常见方式

网站攻击的手段极其多样，但是黑客常用的网站攻击手段主要有DoS攻击、DDoS攻击、SQL注入攻击等。

实战1：网站的DoS攻击

DoS（Denial of Service，拒绝服务攻击）攻击主要是企图通过强占网站服务器中的存储空间资源，使网站服务器崩溃或资源耗尽，进而无法对外继续提供服务的一种攻击方式。使用DoS攻击，实现对方服务器拒绝服务攻击，其原理有以下两点。

（1）迫使服务器的缓冲区爆满，不能接收新的请求。

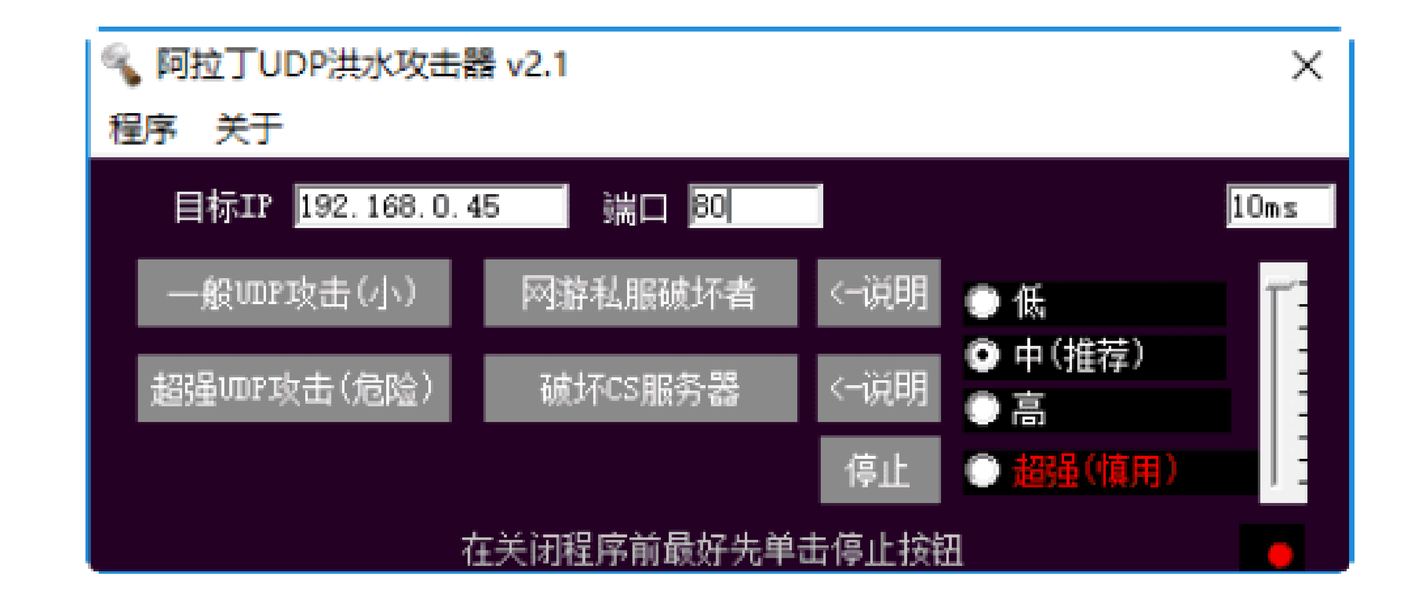
（2）使用IP欺骗，致使服务器把合法用户的连接复位，影响合法用户的链接。

对目标主机实施DoS攻击，首先对攻击目标的网络带宽有很高的要求，因为只有足够的带宽，才可以发送足够破坏防火墙的数据，使用DoS攻击工具可以轻松实现攻击。

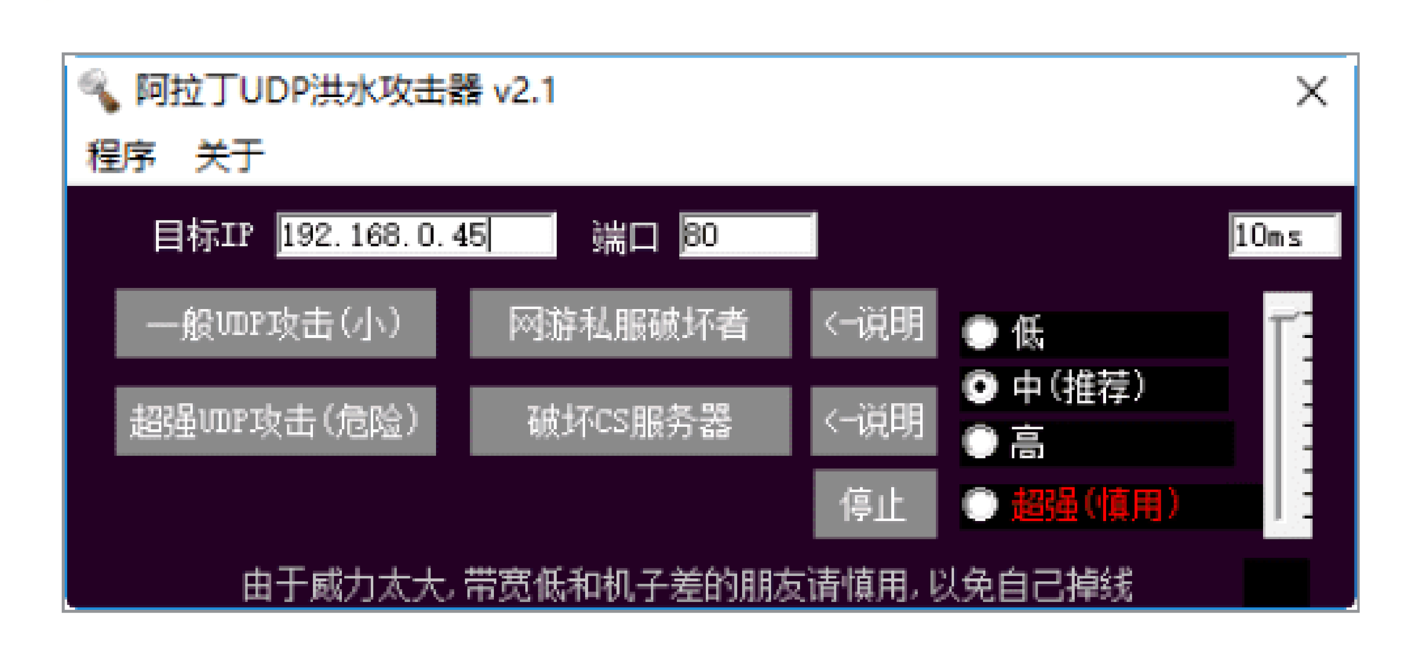
这里介绍一款常见的DoS攻击工具——阿拉丁UDP洪水攻击器，该工具是一个威力巨大的UDP洪水攻击软件。其界面非常简单，只需要输入要攻击网站服务器的IP地址和端口，单击相应的按钮即可进行UDP洪水攻击。

使用阿拉丁UDP洪水攻击器的具体步骤如下。

Step 01 下载并运行阿拉丁UDP洪水攻击器，在“目标IP”文本框中输入要攻击网站的服务器的IP地址；在“端口”文本框中输入要攻击的目标端口，如下图所示。



Step 02 设置完毕后，单击“一般UDP攻击（小）”按钮，即可进行UDP洪水攻击。阿拉丁UDP洪水攻击器提供了4种UDP洪水攻击方式，即“一般UDP攻击（小）”“网游私服破坏者”“超强UDP攻击（危险）”以及“破坏CS服务器”。其中“超强UDP攻击”方式的危害最大，一般不要使用这种方式。



实战2：网站的DDoS攻击

DDoS是Distributed Denial of Service的简称，意思是分布式拒绝服务攻击，很多DoS攻击源一起攻击某台服务器就组成了DDoS攻击。

1. DDoS攻击的常见方式

目前网络上以分布式拒绝服务实施攻击较多，下面介绍几种常见的DDoS攻击。

（1）SYN变种攻击。发送伪造源IP的SYN数据包，但数据包不是64字节，而是上千字节。这种攻击会造成一些防火墙处理错误锁死，消耗服务器CPU内存的同时还会堵塞带宽。

（2）TCP混乱数据包攻击。发送伪造源IP的 TCP数据包，TCP头的TCP Flags 部分混乱的可能是syn、ack、syn+ack、syn+rst等，会造成一些防火墙处理错误锁死，消耗服务器CPU内存的同时还会堵塞带宽。

（3）针对UDP协议的攻击。很多聊天室与视频音频软件均通过UDP数据包传输，攻击者针对要攻击的网络软件协议，发送和正常数据一样的数据包，这种攻击非常难防护，一般防火墙通过拦截攻击数据包的特征码防护，但这样会造成正常的数据包也会被拦截。

（4）针对Web Server的多连接攻击：通过控制大量主机同时连接访问网站，造成网站无法处理、瘫痪，这种攻击和正常访问网站是一样的，只是瞬间访问量增加几十倍甚至上百倍，有些防火墙可通过限制每个连接过来的IP连接数来防护，但这样会造成正常用户稍微多打开几次网站也会被封。

（5）针对Web Server的变种攻击。通过控制大量主机同时连接访问网站，一旦连接建立就不断开，一直发送一些特殊的GET访问请求，造成网站数据库或者某些页面耗费大量的CPU，这样通过限制每个连接过来的IP连接数就失效了，因为每个主机可能只建立一个或者只建立少量的连接。



（6）针对Web Server的变种攻击。通过控制大量主机同时连接网站端口，但不发送GET请求而是乱七八糟的字符，大部分防火墙分析攻击数据包前三个字节是GET字符，来进行HTTP分析。这种攻击不发送GET请求就可以绕过防火墙到达服务器，一般服务器都是共享带宽的，带宽不会超过10M，所以大量主机攻击数据包就会把这台服务器的共享带宽堵塞，造成服务器瘫痪。这种攻击也非常难防护，因为如果只简单拦截客户端发送过来没有GET字符的数据包，会错误地封锁很多正常的数据包，造成正常用户无法访问。

（7）针对游戏服务器的攻击。因为游戏服务器非常多，所以攻击的种类也花样辈出，大概有几十种之多，而且还在不断地发现新的攻击种类。

2. DDoS攻击的一般步骤

在这里将介绍黑客对目标主机实施DDoS攻击的一般步骤，但是DDoS并不像入侵一台主机那样简单。一般来说，黑客进行DDoS攻击时的操作步骤如下。

（1）搜集了解目标的情况。

在实施DDoS攻击之前，黑客一般都

需要获取被攻击目标主机的数目、地址、配置、性能和带宽等信息。对于DDoS攻击者，在攻击互联网上的某个站点之前，需要先确定到底有多少台主机在支持这个站点。一个大的网站可能有很多台主机利用负载均衡技术提供同一个网站的WWW服务。

如果某网站需要下列的地址来提供相应服务：

66.218.xx.84

66.218.xx.86

66.218.xx.87

66.218.xx.88

66.218.xx.89

若要对该网站进行DDoS攻击，应该攻击哪一个地址呢？如果仅仅使66.218.xx.87这台机器瘫掉，但其他主机还能向外提供WWW服务，而想让别人访问不到该网站，必须使所有这些IP地址的计算机都瘫掉才行。在实际的应用中，一个IP地址往往还代表着数台计算机。网站管理员会使用四层或七层交换机来做负载均衡，把对一个IP地址的访问以特定的算法分配到下属的每个主机上去。此时对于DDoS攻击者情况就更复杂了，其面对的任务是让这几十台主机的服务都不正常。

所以搜集情报对DDoS攻击者非常重要，这关系到使用多少台“傀儡”机才能实现效果的问题。一般情况下，至少需要数百台甚至更多计算机才可以达到满意效果。同时网络带宽越宽，攻击的效果就越好。但在实际过程中，有很多黑客并不进行情报搜集而直接进行DDoS攻击，这时候攻击的盲目性就很大。

（2）占领傀儡机。

黑客可能将链路状态好、性能好、安全管理水平差的主机作为傀儡机，一些安全性比较差的小型站点以及服务器常常是黑客们的首选目标。占领和控制被攻击的主机，得到一个有权限完成DDoS攻击任务的账号，甚至取得最高的管理权限。对于一个DDoS攻击者，准备好一定数量的傀儡机是必须的，下面介绍黑客是如何攻击并占领它们的。

首先，黑客需要做的工作是扫描，利用扫描器去发现互联网上那些有漏洞的机器，如程序的溢出漏洞、CGI、Unicode、FTP、数据库漏洞等都是黑客希望得到的扫描结果。随后就是利用特定的入侵工具尝试入侵目标主机。黑客在占领了一台傀儡机之后，除了留后门擦脚印这些基本工作之外，还会把DDoS攻击用的程序利用FTP工具上传到目标傀儡机上。在攻击机上，会有一个DDoS的发包程序，黑客就是利用它来向受害目标发送恶意攻击包的。黑客在傀儡机上安装DDoS攻击程序，包括攻击服务器和攻击执行器两种。

（3）实际攻击。

经过前面的精心准备之后，黑客就开始向目标主机实施DDoS攻击。如果前面的准备做得好，实际攻击过程反而比较简单。黑客登录到作为控制台的傀儡机，向所有的攻击机发出攻击的命令。此时埋伏在攻击机中的DDoS攻击程序就会响应控制台的命令，会向受害主机以高速度发送大量的数据包，导致死机或是无法响应正常的请求。

黑客一般会以远远超出受害方处理能力的速度进行攻击。有的攻击者一边攻击，一边还会用各种手段来监视攻击的效果，在必要时进行一些调整。如可以不断地ping目标主机，在能接到回应时，就再加大一些流量或使用更多的傀儡机来进行攻击。

3. 使用工具进行DDoS攻击

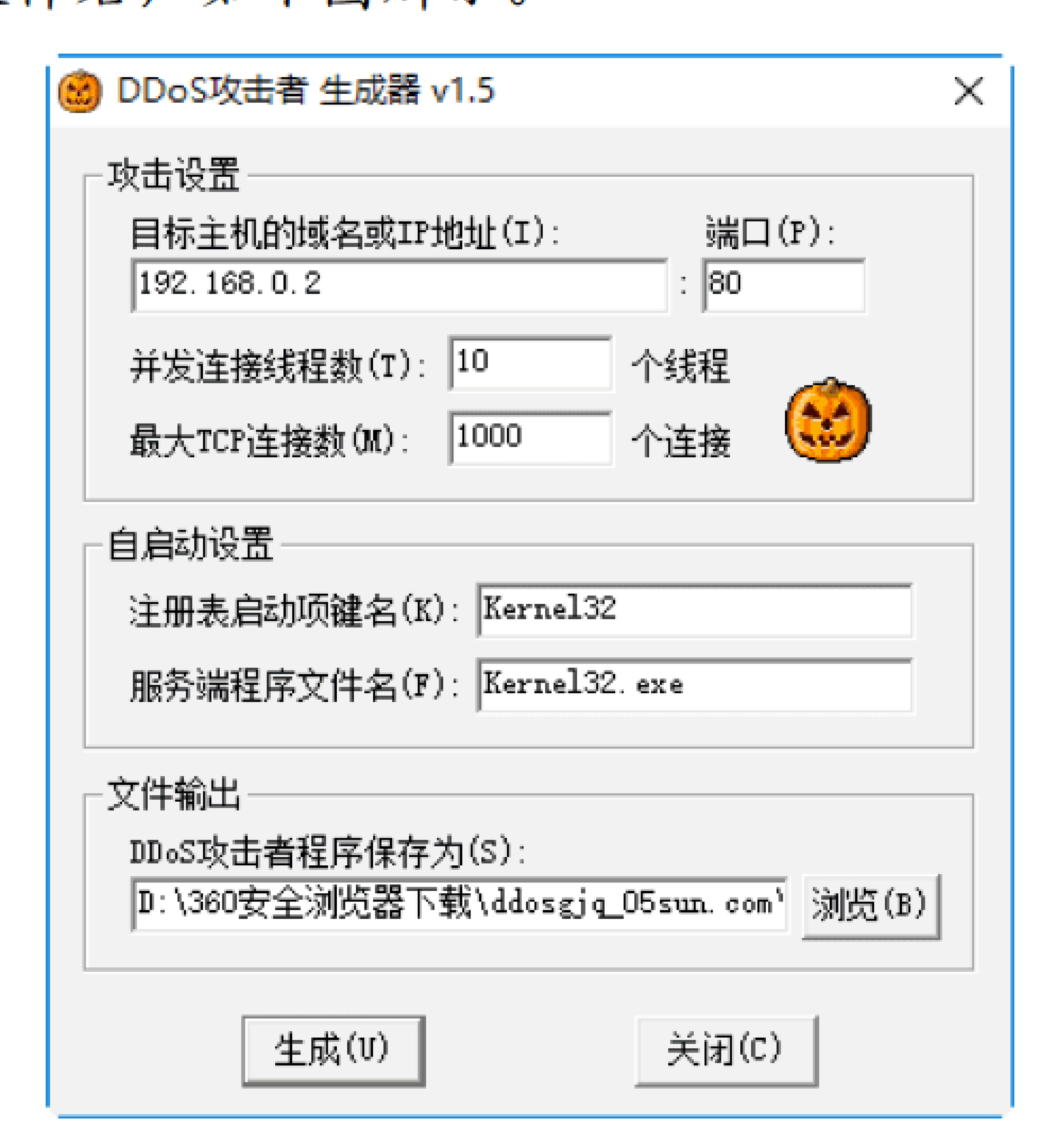
DDoS攻击方式比DoS攻击危害性更大，使用工具可以进行DDoS攻击，下面将介绍一款常见的DDoS攻击工具——DDoS攻击者。

DDoS攻击者是一个有名的DDoS攻

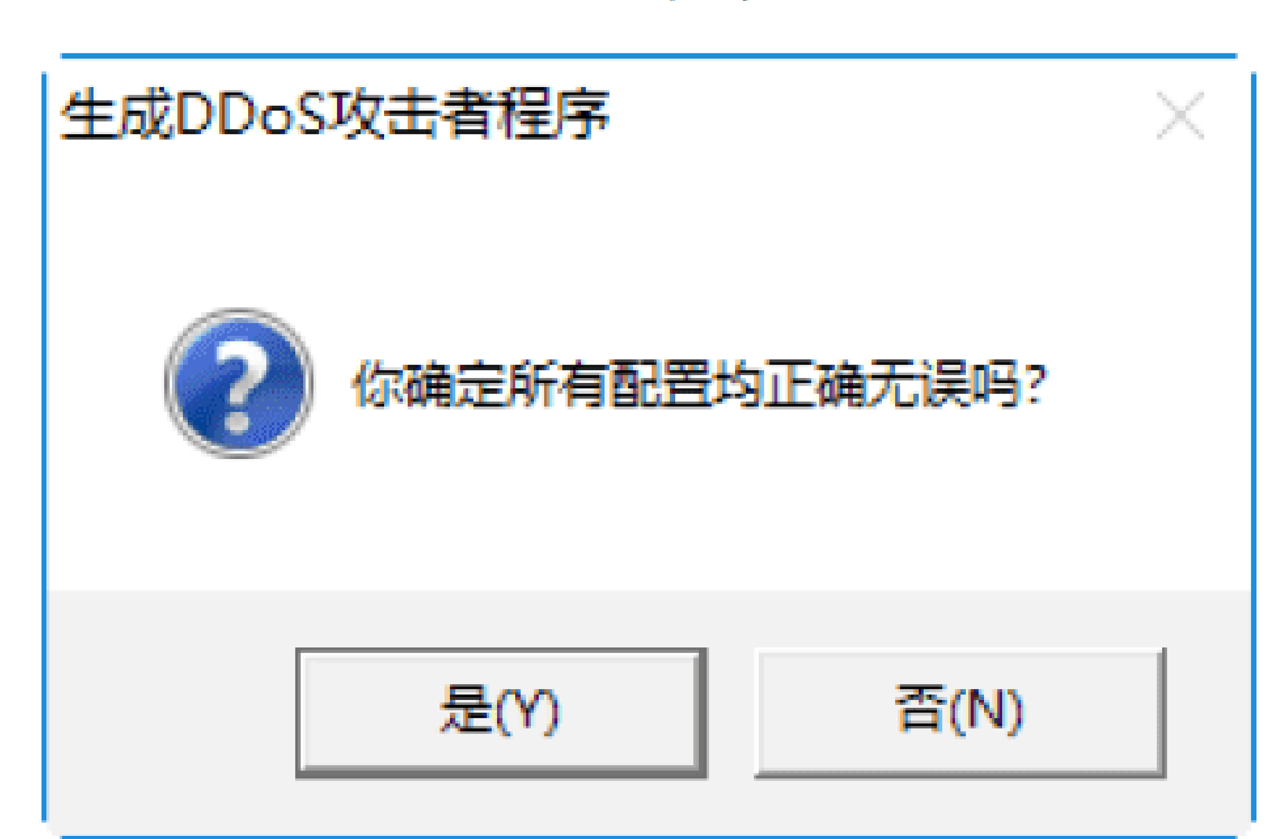
击工具，由于采用了与其他同类软件不同的攻击方法，所以效果更好。程序运行后可自动驻入系统，并在以后随系统启动而启动，上网时自动对设定好的目标进行攻击，还可自由设置“并发连接线程数”“最大TCP连接数”等参数。

使用DDoS攻击者进行攻击的具体操作步骤如下。

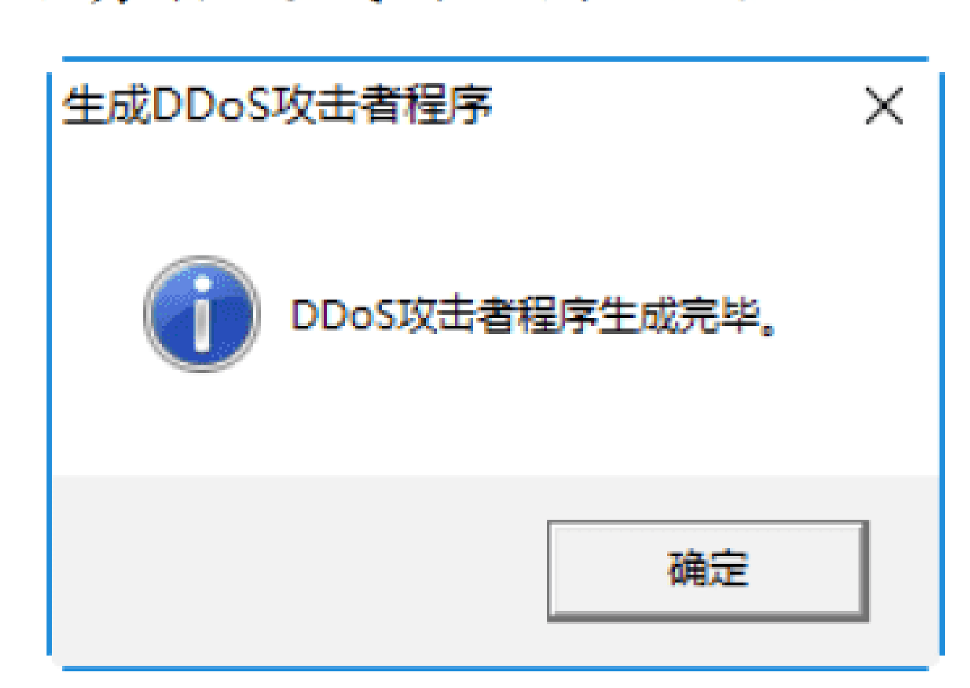
Step 01 下载并启动DDoS攻击工具，在“目标主机的域名或IP地址”文本框中输入要攻击主机的域名或IP地址，建议用域名，因为IP地址是经常变的；在“自启动设置”栏目中输入注册表启动项键名与服务器端程序文件名，如下图所示。



Step 02 单击“生成”按钮，即可打开“你确定所有配置均正确无误吗？”提示框，单击“是”按钮，如下图所示。



Step 03 打开“DDoS攻击者程序生成完毕”提示框，单击“确定”按钮，即可生成一个DDoSer.exe的自动攻击程序，如下图所示。把这个攻击程序散布到其主机上运行，只要运行了DDoS攻击者程序，就会立即开始攻击指定的IP地址，同时运行的人越多，对服务器造成的压力就越大。



实战3：网站的SQL注入攻击

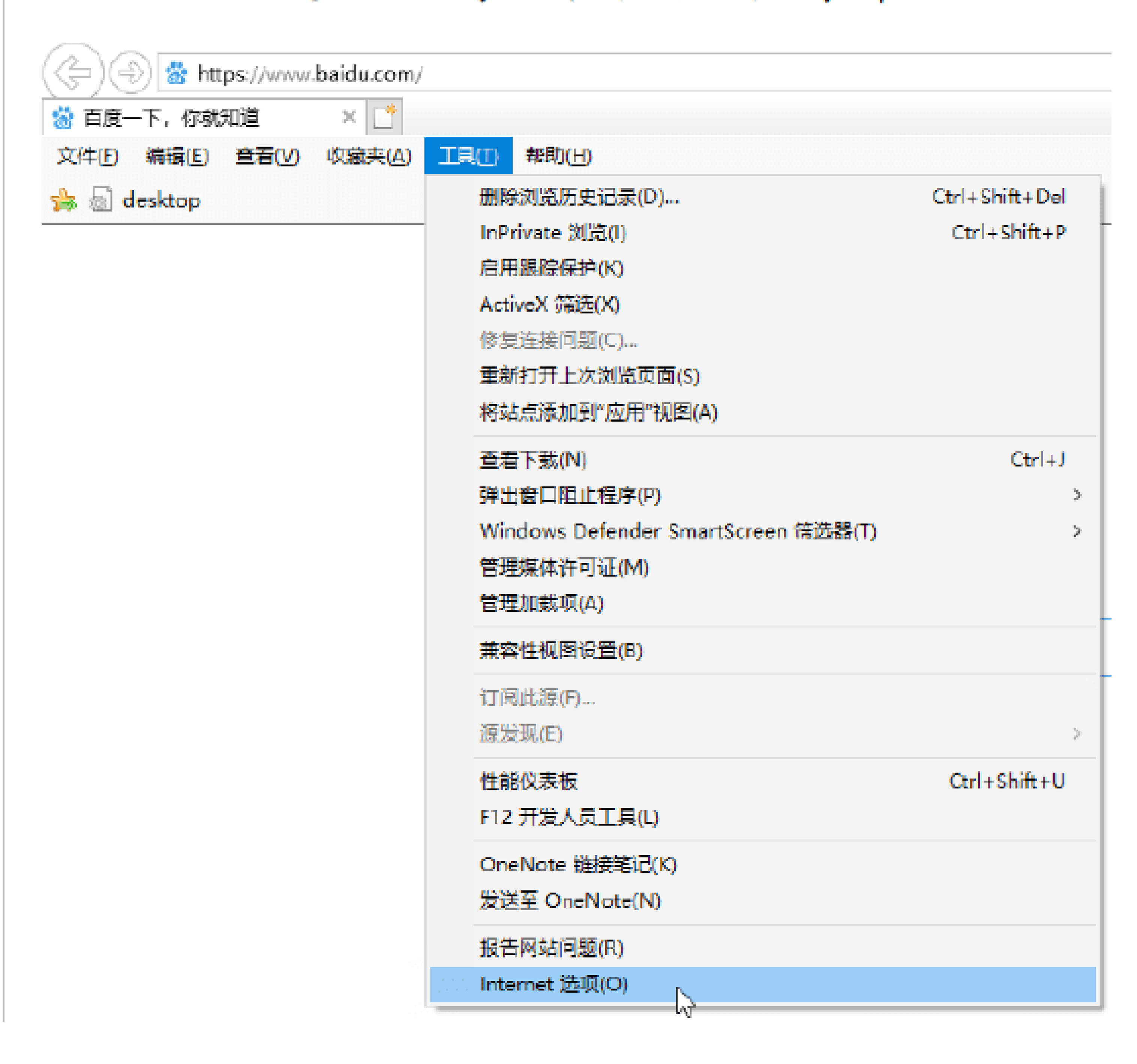


所谓SQL注入是通过把SQL命令插入到Web表单递交，输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令的目的。

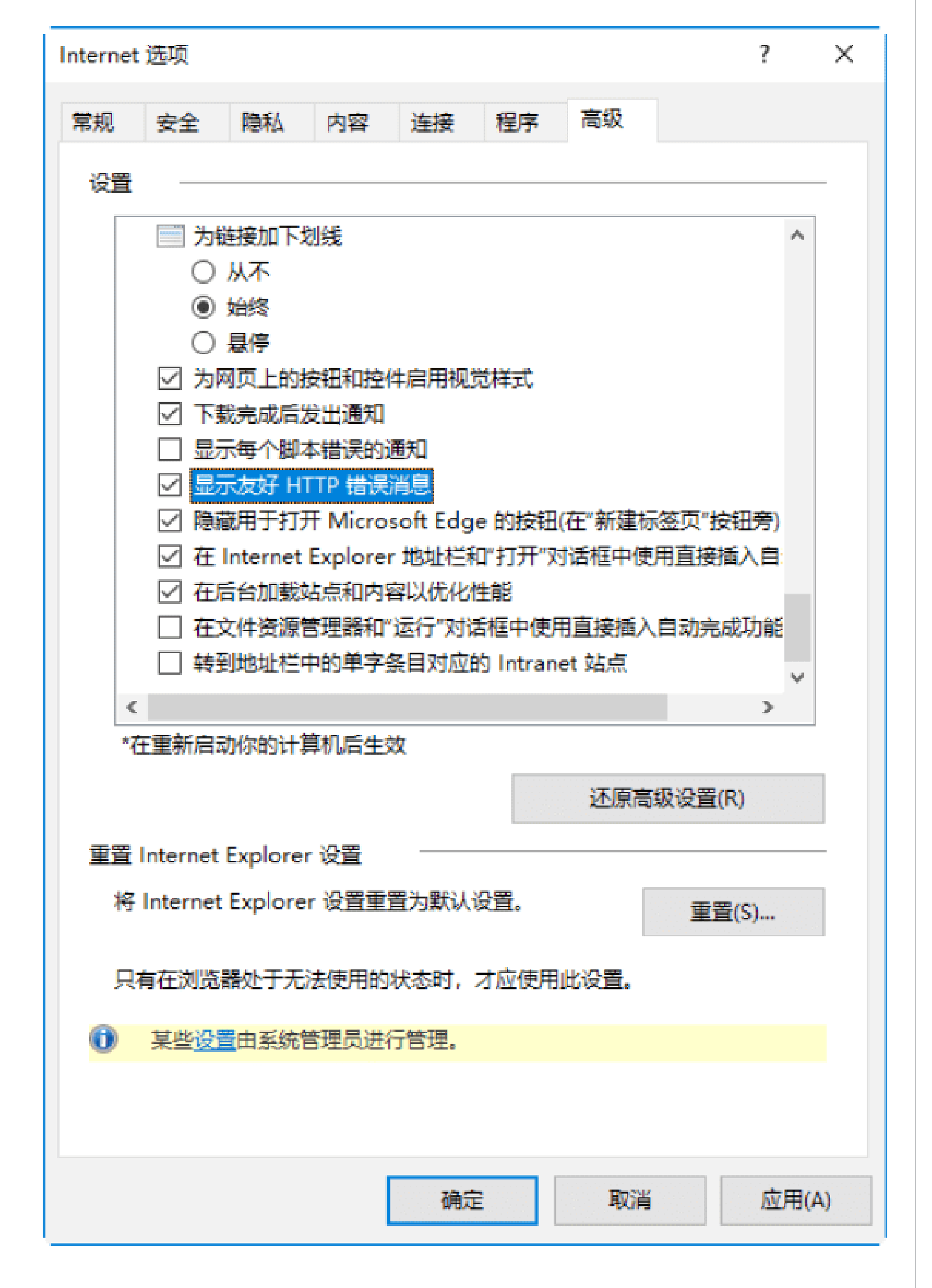
1. SQL注入攻击前的准备

在进行SQL注入入侵时，需要利用从服务器上返回各种出错信息，但在浏览器中默认设置时不显示详细错误返回信息，所以通常只能看到“HTTP 500服务器错误”提示信息。因此，需要在进行SQL注入攻击之前先设置IE浏览器。具体的设置步骤如下。

Step 01 在IE浏览器窗口，选择“工具”→“Internet选项”选项，即可打开“Internet选项”对话框，如下图所示。



Step 02 选择“高级”选项卡，勾选“显示友好HTTP错误信息”复选框，单击“确定”按钮，即可完成设置，如下图所示。



2. SQL注入漏洞扫描器

ASP环境的注入扫描器有WIS+WED、NBSI、冰舞等，其中冰舞是一款针对ASP脚本网站的扫描工具。它结合扫描和注射为一体，能够很全面地寻找目标网站存在的漏洞。其主窗口如下图所示。

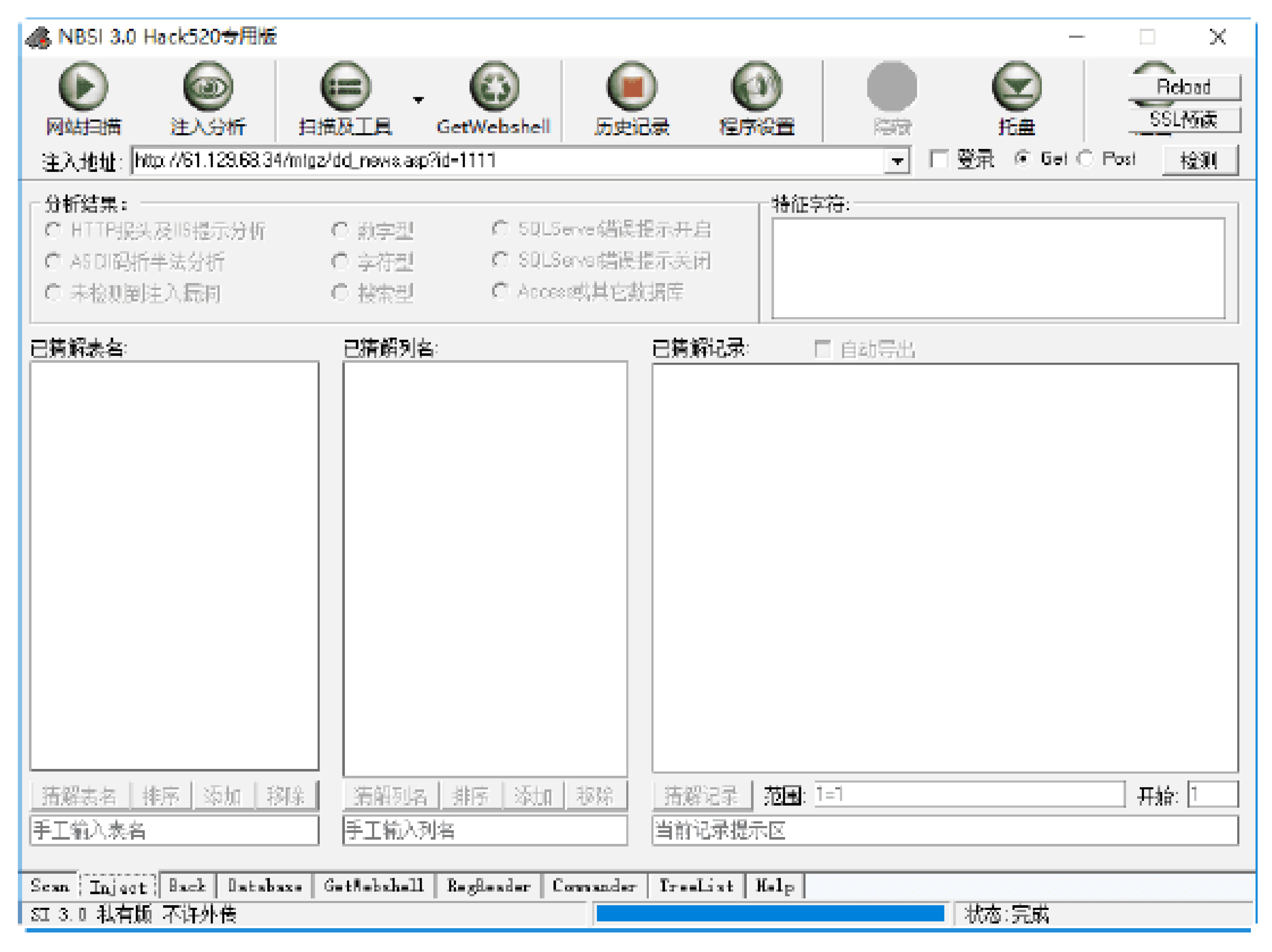


3. 用NBSI实施注入攻击

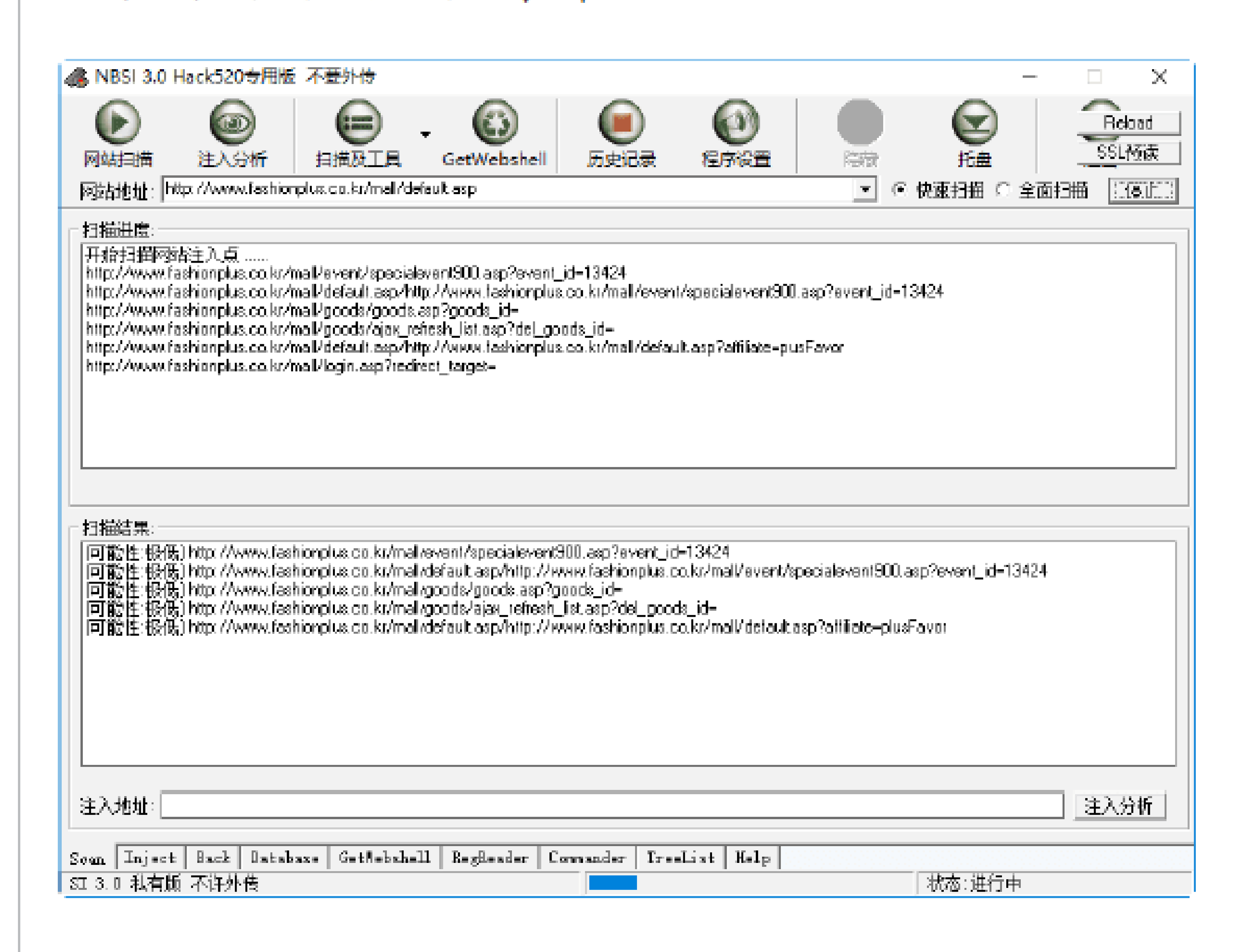
随着网络技术的不断发展，现在涌现出大量的专门对数据库文件进行探测的工具，如HDSI、NBSI、SQL注入工具等，通过这些工具可以快速在网站的大量文件中找到需要的数据库文件路径。

这里以NBSI工具为例，其探测网站数据库文件路径的具体操作步骤如下。

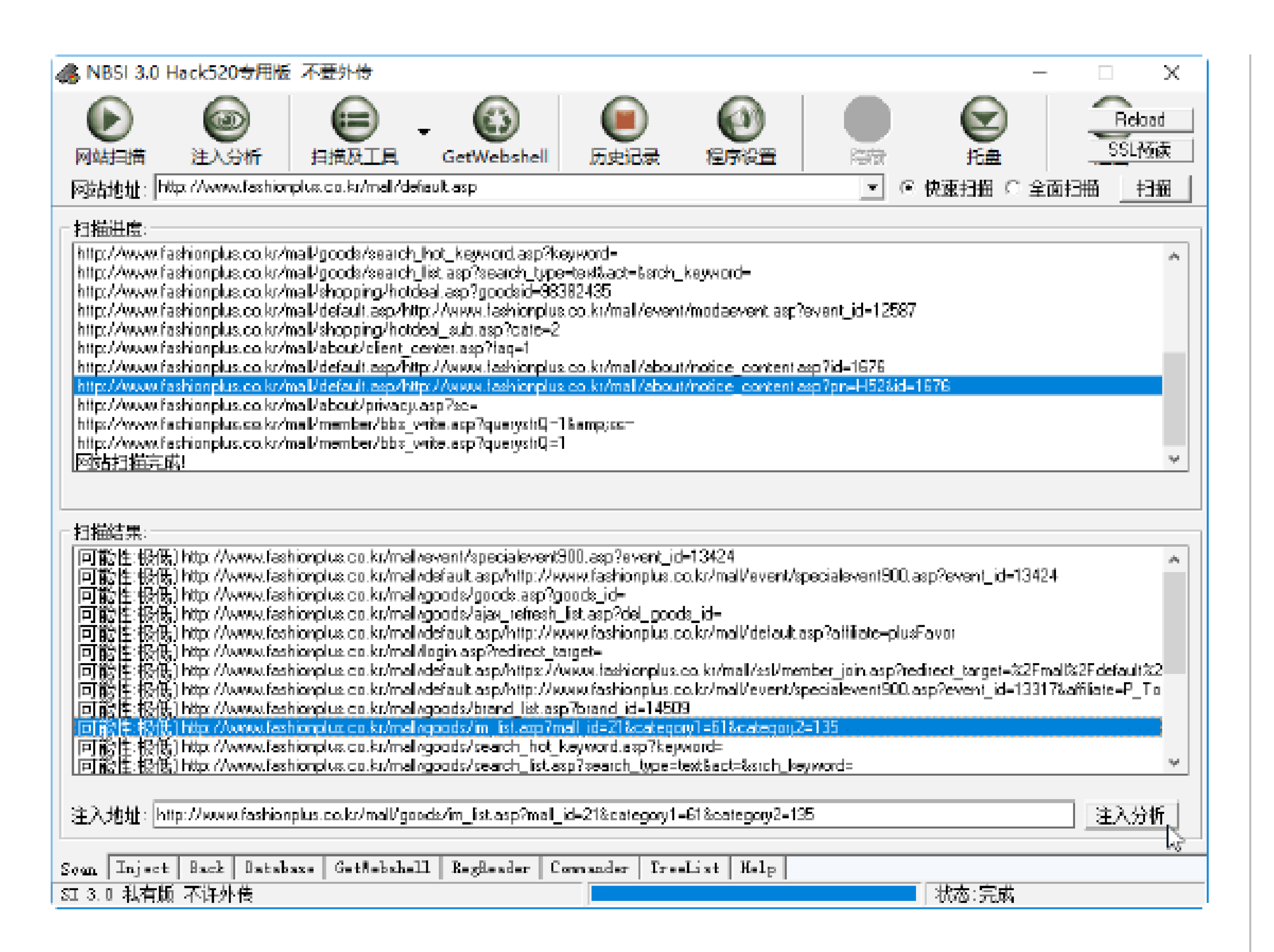
Step 01 下载并解压缩NBSI3.0文件，双击其中的可执行文件图标，即可打开NBSI主窗口，如下图所示。



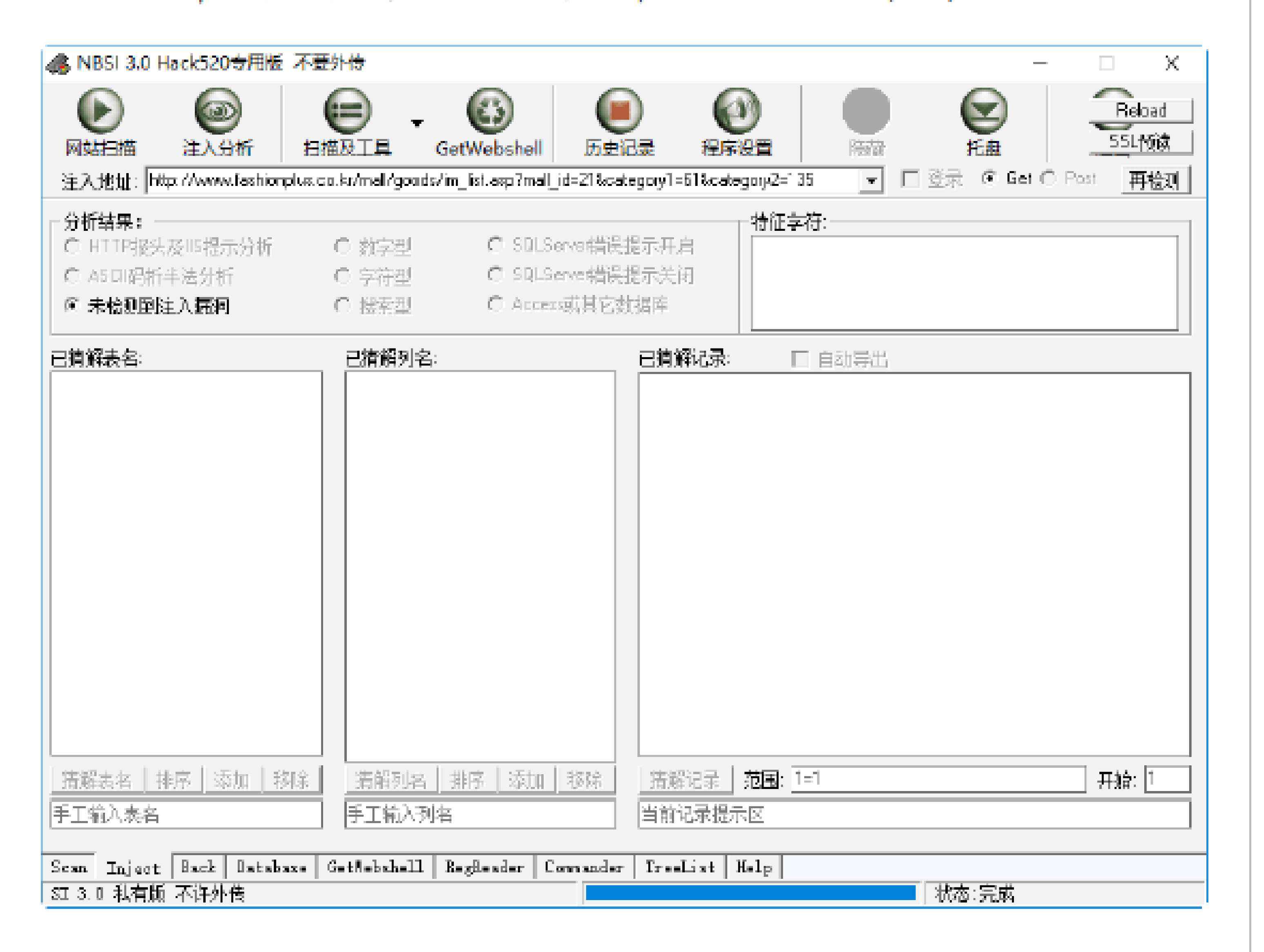
Step 02 在网站地址文本框中输入要进行注入攻击的网址，并选中“快速扫描”单选按钮，单击“扫描”按钮，即可进行网站注入点扫描，如下图所示。



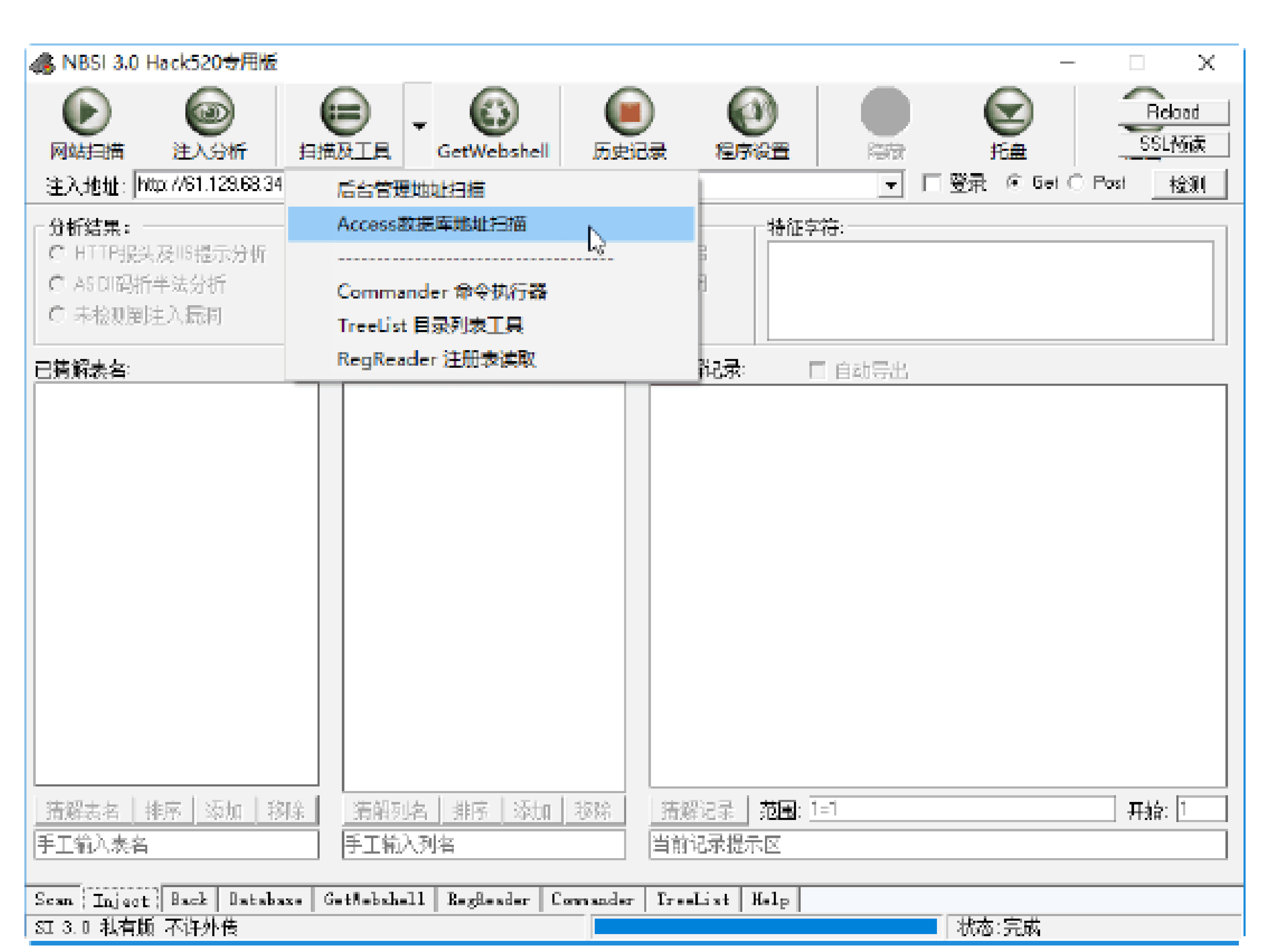
Step 03 扫描完成后，在扫描结果中选择一个注入点网址，如下图所示。



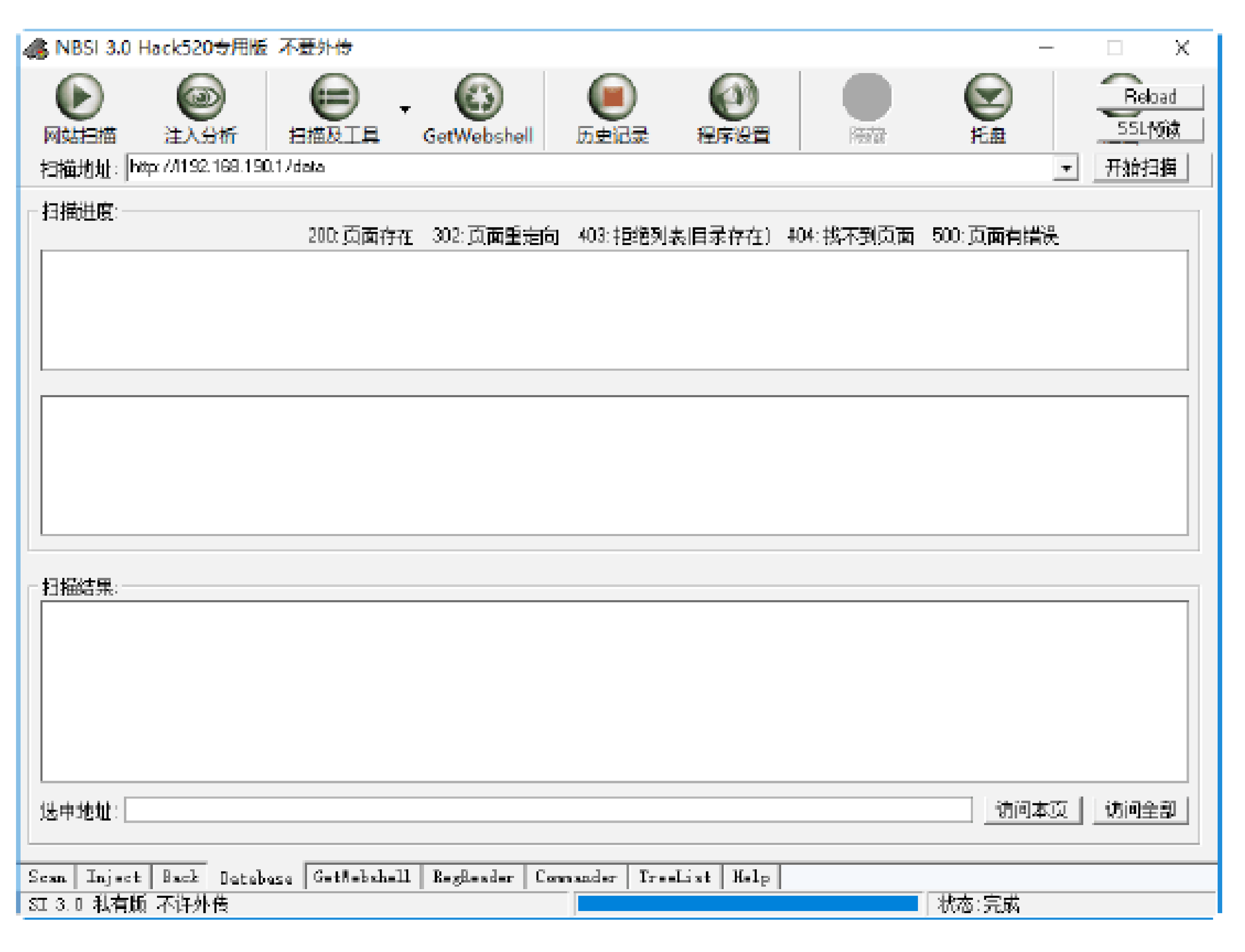
Step 04 单击“注入分析”按钮，即可进入“注入分析”工作界面，单击“检测”按钮，即可进行注入分析，如下图所示。



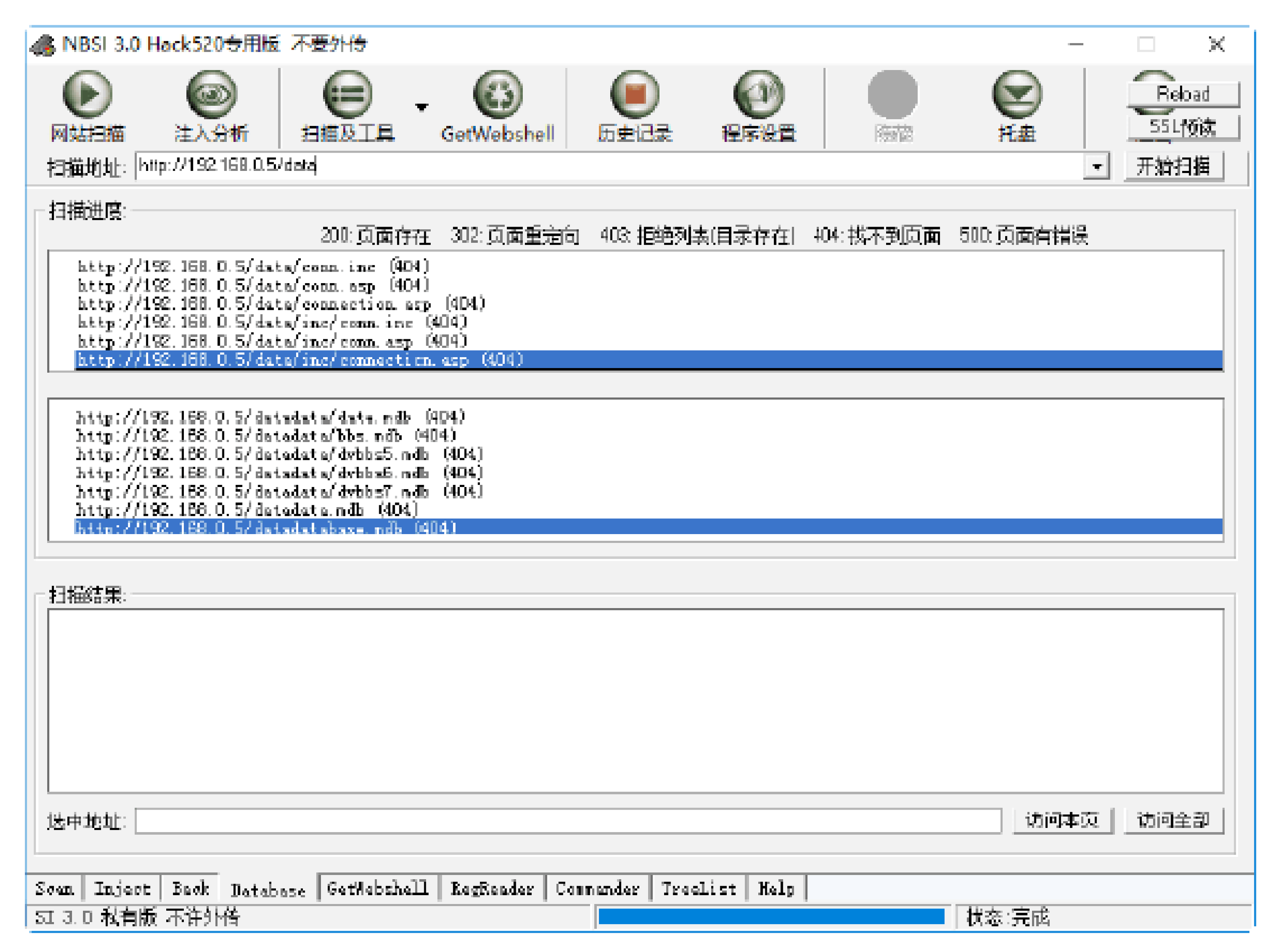
Step 05 在NBSI主窗口中单击“扫描及工具”按钮右侧的下拉箭头，在弹出的快捷菜单中选择“Access数据库地址扫描”选项，如下图所示。



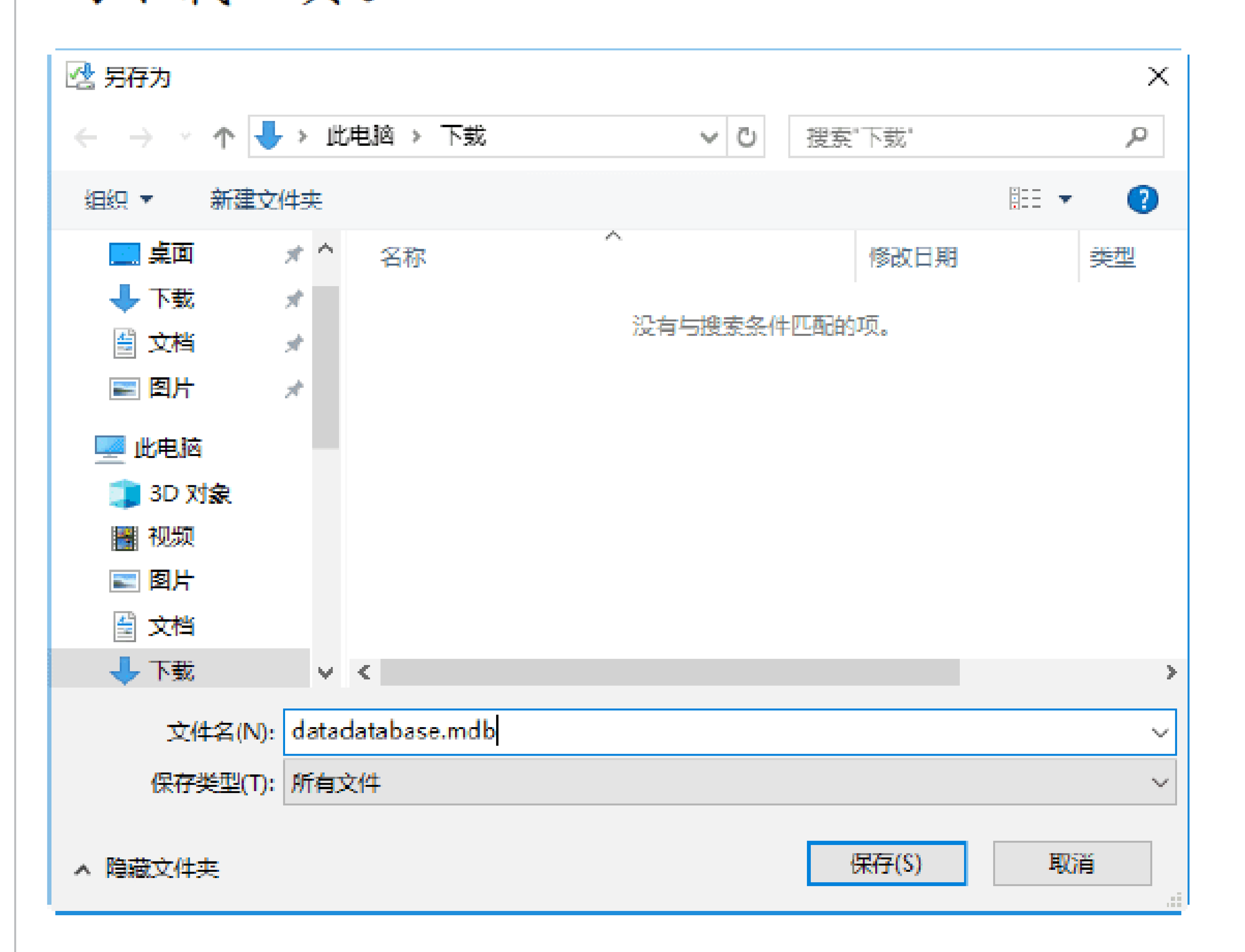
Step 06 在打开的设置界面中的“扫描地址”文本框中输入要扫描的远程网站地址或数据库文件夹名称，如下图所示。



Step 07 单击“开始扫描”按钮，即可将mdb数据库文件的路径扫描出来，如下图所示。

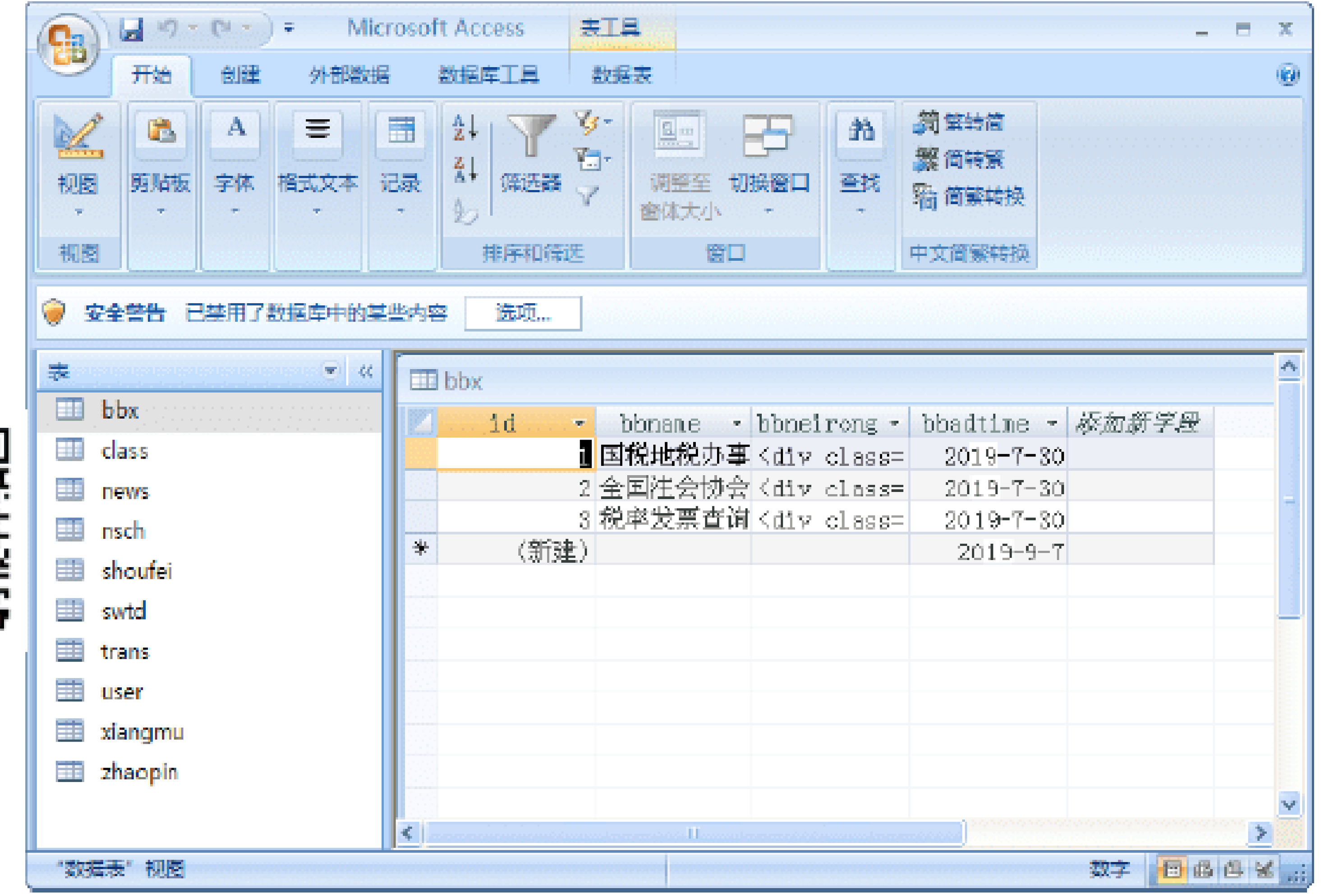


Step 08 将扫描出来的数据库路径进行复制，将该路径粘贴到IE浏览器的地址栏中，即可自动打开浏览器下载功能，并弹出“另存为”对话框，如下图所示，或使用其他的下载工具。



Step 09 单击“保存”按钮，即可将该数据

下载到本地磁盘中，打开后结果如下图所示，这样，就掌握了网站的数据库，实现了SQL注入攻击。



11.4　网站系统的安全防护

在了解了攻击网站常用的手段后，用户就可以有针对性地对网站攻击进行安全防御，以增强网站服务器的安全性。



实战4：网站硬件的安全防护

硬件中最主要的就是服务器，一般要求使用专用的服务器，不要使用PC代替。因为专用的服务器中有多个CPU，并且硬盘的各方面的配置也比较优秀；如果其中一个CPU或硬盘坏了，别的CPU和硬盘还可以继续工作，不会影响到网站的正常运行。

网站机房通常要注意室内的温度、湿度以及通风性，这些将影响到服务器的散热和性能的正常发挥。如果有条件，最好使用两台或两台以上的服务器，所有的配置最好都是一样的，因为服务器经过一段时间要进行停机检修，在检修的时候可以运行别的服务器工作，这样不会影响到网站的正常运行，如下图所示为网站服务器的工作环境。



实战5：网站软件的安全防护

软件管理也是确保一个网站能够良好运行的必要条件，通常包括服务器的操作系统配置、网站的定期更新、数据的备份以及网络安全的防护等。

1. 服务器的操作系统配置

一个网站要能正常运行，硬件环境是一个先决条件。但是服务器操作系统的配置是否可行和设置的优良性如何，则是一个网站能否良好长期运行的保证。除了要定期对这些操作系统进行维护外，还要定期对操作系统进行更新，并使用最先进的操作系统。

2. 网站的定期更新

网站的创建并不是一成不变的，还要对网站进行定期的更新。除了更新网站的信息外，还要更新或调整网站的功能和服务。对网站中的废旧文件要随时清除，以提高网站的精良性，从而提高网站的运行速度。另外，就是要时时关注互联网的发展趋势，随时调整自己的网站，使其顺应潮流，以便给别人提供更便捷和贴切的服务。

3. 数据的备份

所谓数据的备份，就是对自己网站中的数据进行定期备份，这样既可以防止服务器出现突发错误丢失数据，又可以防止自己的网站被别人“黑”掉。如果有了定期的网站数据备份，那么即使自己的网站被别人“黑”掉了，也不会影响网站的正常运行。

4. 网络安全的防护

所谓网络的安全防护，就是防止自己的网站被别人非法地侵入和破坏。除了要对服务器进行安全设置外，首要的一点是要注意及时下载和安装软件的补丁程序。另外，还要在服务器中安装、设置防火墙。防火墙虽然是确保安全的一个有效措施，但不是唯一的，也不能确保绝对安全。为此，还应该使用其他的安全措施。

另外一点就是要时刻注意病毒的问题，要时刻对自己的服务器进行查毒、杀毒等操作，以确保系统的安全运行。如下图所示为360杀毒软件的下载页面，下载之后，将其安装到网站服务器中，就可以使用该软件保护系统安全了。



实战6：DDoS攻击的防御措施

随着论坛社区BBS、电子商务、音乐网站、电影网站等网站服务器越来越普及，往往会遭受竞争对手或打击报复者的恶意DDoS攻击，持续的攻击会导致大量用户流失，严重的甚至因人气全失而被迫关闭服务器。

DDoS攻击是黑客最常用的攻击手段，下面列出一些常规的防御措施。

（1）定期扫描。要定期扫描现有的网络主节点，清查可能存在的安全漏洞，对新出现的漏洞及时进行修补。骨干节点上计算机因为具有较高的带宽，是黑客利用的最佳位置，所以对这些主机本身加强安全是非常重要的。连接到网络主节点的都是服务器级别的计算机，所以定期扫描漏洞就非常重要了。

（2）在骨干节点配置防火墙。防火墙（如金盾抗DDoS防火墙、傲盾软件的傲盾防火墙等）本身能抵御DDoS攻击和其他一些攻击。在发现受到攻击时，可以将攻击导向一些“傀儡”主机，以保护真正的主机不被攻击。

（3）用足够的机器承受黑客攻击。这是一种较为理想的应对方案，如果用户拥有足够的容量和资源给黑客攻击，在它不断访问用户、夺取用户资源之时，自己的能量也在逐渐耗失，或许未等用户被攻死，黑客已无力应对。不过此方法需要投入的资金比较多，平时大多数设备处于空闲状态，和目前中小企业网络实际运行情况不相符。

（4）充分利用网络设备保护网络资源。网络设备是指路由器、防火墙等负载均衡设备，可将网络有效地保护起来。当网络被攻击时，最先死掉的是路由器，其他机器没有死。死掉的路由器经重启后会恢复正常，而且启动起来还很快，不会造成太大损失。若其他服务器死掉，其中的数据会丢失，而且重启服务器又是一个漫长过程。特别是一个公司使用了负载均衡设备，当一台路由器被攻击死机时，另一台将马上工作，从而最大程度削减了DDoS的攻击。



（5）过滤不必要的服务和端口。可使用Inexpress、Express、Forwarding等工具来过滤不必要的服务和端口，即在路由器上过滤假IP。只开放服务端口成为目前很多服务器的流行做法，如WWW服务器只开放80，而将其他所有端口关闭或在防火墙上做阻止策略。

（6）检查访问者的来源。使用Unicast Reverse Path Forwarding等通过反向路由器查询的方法，检查访问者的IP地址是否是真，如果是假将加以屏蔽。许多黑客攻击常采用假IP地址方式迷惑用户，很难查出它

来自何处。因此，利用Unicast Reverse Path Forwarding可降低假IP地址出现的概率，有助于提高网络安全性。

（7）过滤所有RFC1918 IP地址。RFC1918 IP地址是内部网的IP地址，如10.0.0.0、192.168.0.0，它们不是某个网段的固定的IP地址，而是因特网内部保留的区域性IP地址，应该把它们过滤掉。此方法并不是过滤内部员工的访问，而是过滤攻击时伪造的大量虚假内部IP，以预防DDoS攻击。



（8）限制SYN/ICMP流量。用户应在路由器上配置SYN/ICMP的最大流量来限制SYN/ ICMP封包所能占有的最高频宽，这样，当出现大量超过所限定的SYN/ICMP流量时，说明不是正常的网络访问，而是有黑客入侵。早期通过限制SYN/ICMP流量是最好的防范DoS方法，虽然目前该方法对于DDoS效果不太明显了，不过仍然能够起到一定的作用。

但如果用户正在遭受攻击，那他所能做的抵御工作将是非常有限的。因为在原本没有准备好的情况下，有大流量的攻击冲向用户，很可能在用户还没回过神时，网络系统已经瘫痪。

此时，用户还是可以采取如下几种措施来寻求一线希望。

（1）检查攻击来源。通常黑客会通过很多假IP地址发起攻击，此时，用户若能够分辨出哪些是真IP哪些是假IP地址，了解这些IP来自哪些网段，再找网络管理员将这些机器关闭，从而可以在第一时间消除这些攻击。如果发现这些IP地址是来自外面而不是内部的IP，可以采取过滤的方法，将这些IP地址在服务器或路由器上过滤掉。

（2）找出攻击者所经过的路由，把攻击屏蔽掉。若黑客从某些端口发动攻击，用户可把这些端口屏蔽掉，以阻止入侵。不过此方法对于公司网络出口只有一个，而又遭受到来自外部的DDoS攻击时不太有用，毕竟将出口端口封闭后，所有计算机都无法访问因特网了。

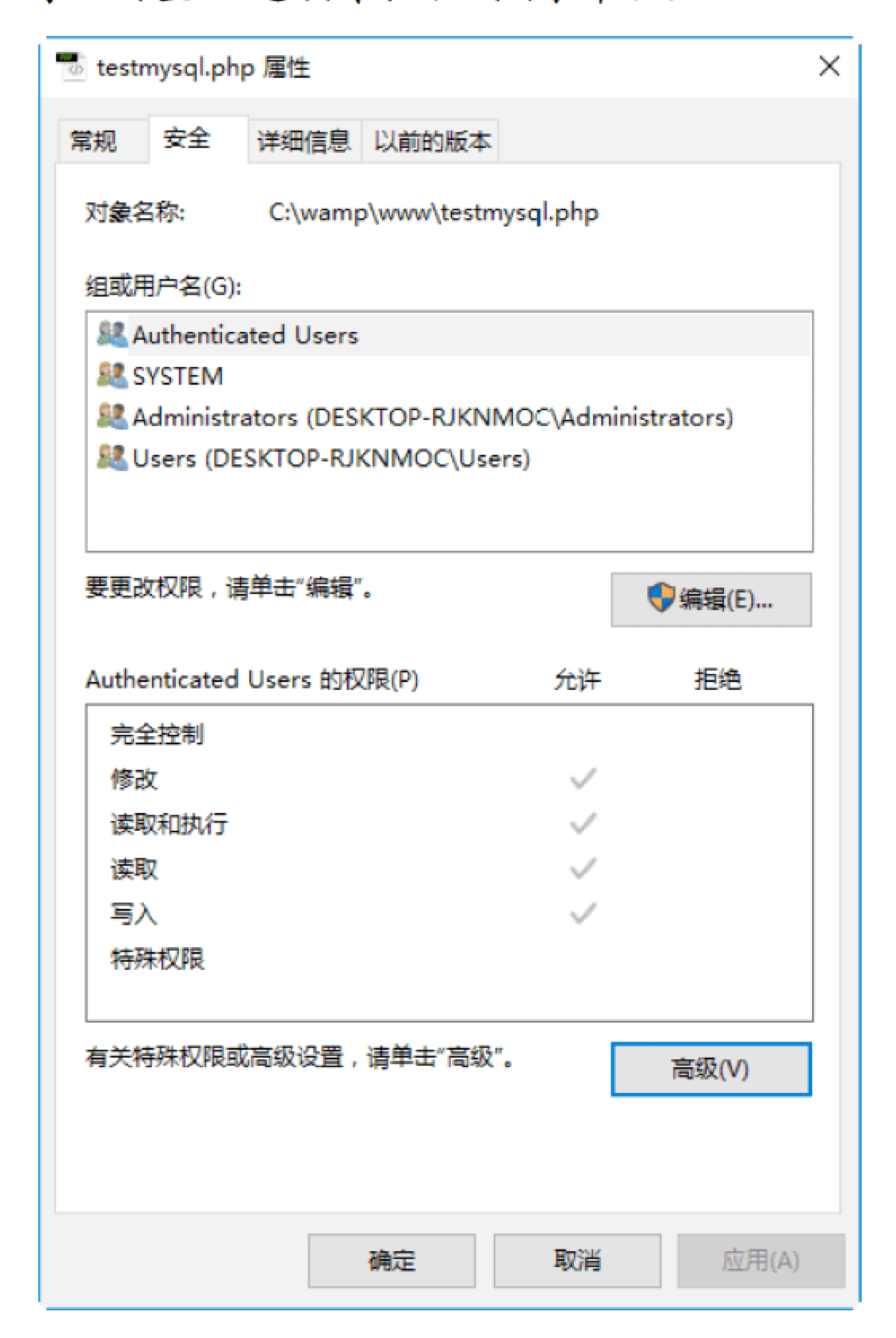
（3）在路由器上滤掉ICMP。虽然在攻击时无法完全消除入侵，但过滤掉ICMP后可有效防止攻击规模的升级，也可以在一定程度上降低攻击的级别。

目前，网络安全界对于DDoS的防范主要还是靠平时维护和扫描来对抗。简单通过软件防范的效果非常不明显，即便是使用了硬件安防设施，也仅仅能起到降低攻击级别的效果，DDoS攻击只能被减弱，无法被彻底消除。

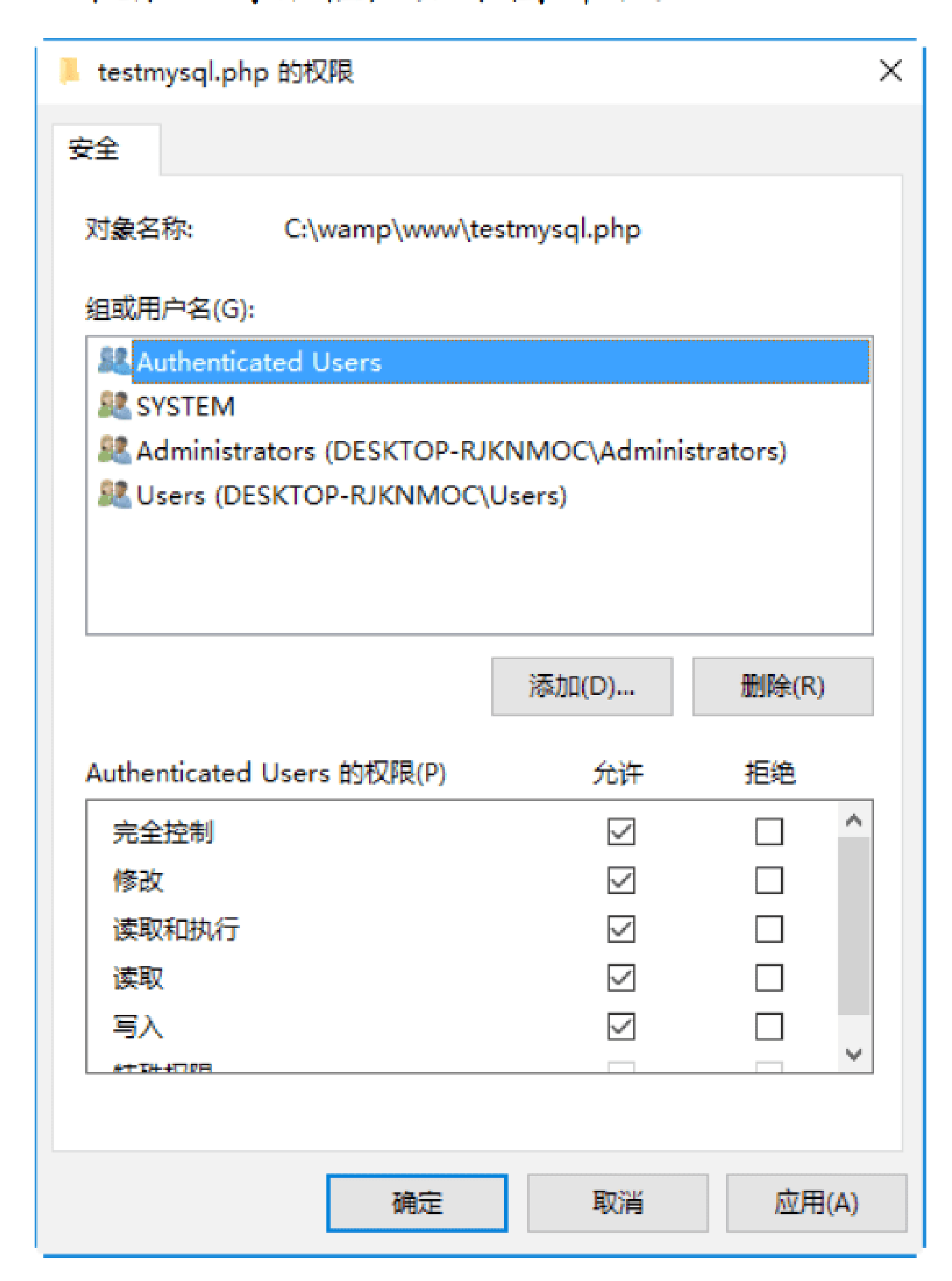
实战7：设置网站的访问权限

限制用户的网站访问权限往往可以有效堵住入侵者的上传，设置网站访问权限的具体操作步骤如下。

Step 01 在资源管理器中右击D:\inetpub中的www.***.com目录，在弹出的快捷菜单中选择“属性”选项，在打开的对话框中切换到“安全”选项卡，如下图所示。

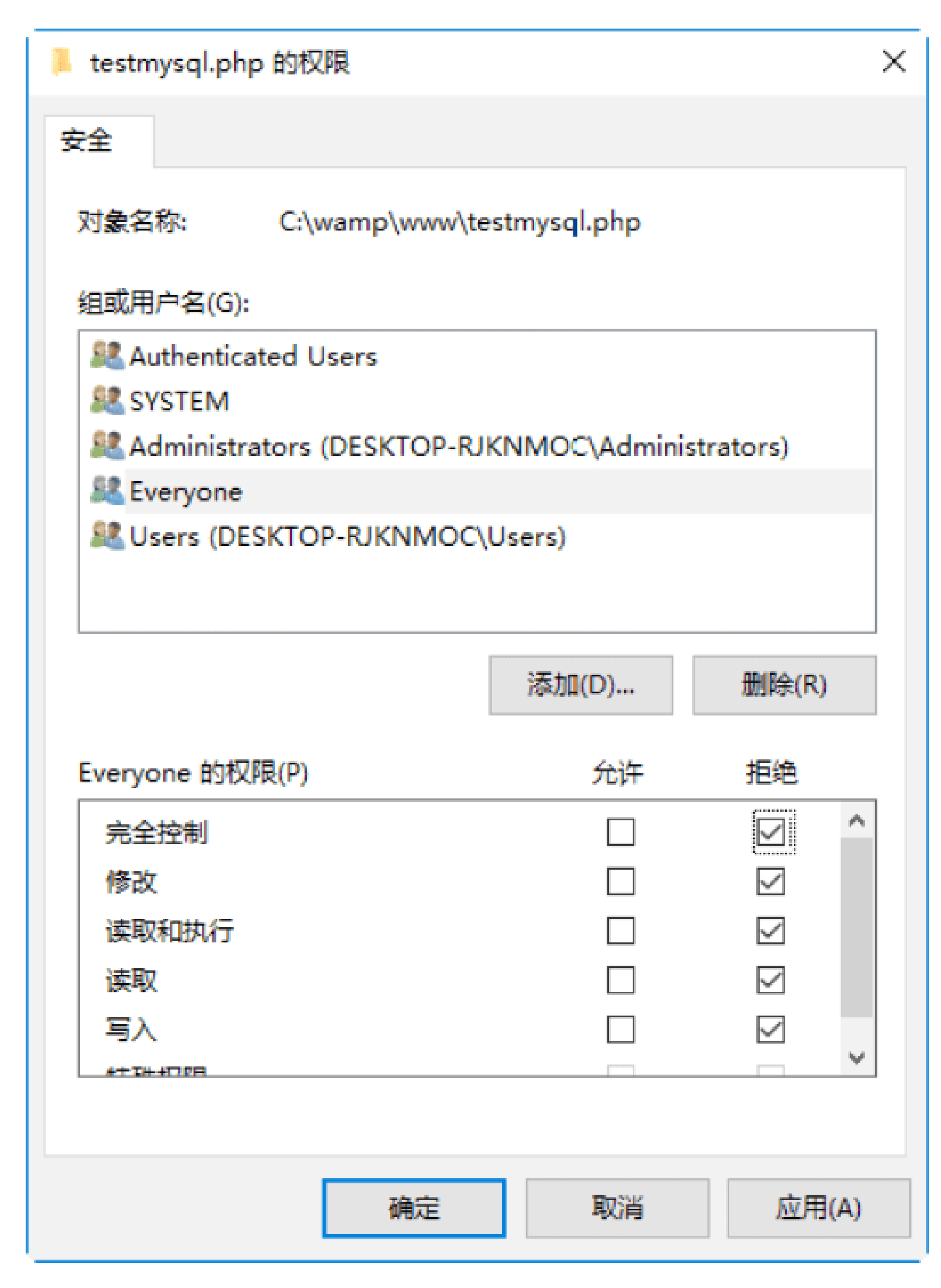


Step 02 在“组和用户名”列表中选择任意一个用户名，然后单击“编辑”按钮，打开“权限”对话框，如下图所示。



Step 03 单击“添加”按钮，打开“选择用户或组”对话框，在“输入对象名称来选择（示例）”文本框中输入用户名Everyone，如下图所示。

Step 04 单击“确定”按钮，返回“权限”对话框，可看到已将Everyone用户添加到列表中。在权限列表中选择“读取和执行”“列出文件夹目录”“读取”权限后，单击“确定”按钮，即可完成设置，如下图所示。



另外，在网页文件夹中还有数据库文件的权限设置需要进行特别设置。因为用户在提交表单或注册等操作时，会修改数据库的数据，所以除了给用户读取的权限外，还需要写入和修改权限，否则会出现用户无法正常访问网站的问题。

设置网页数据库文件的权限的操作方法如下：右击文件夹中的数据库文件，在弹出的快捷菜单中选择“属性”选项，在打开的属性对话框中切换到“安全”选项卡，在“组或用户名称”列表中选择Everyone用户，在“权限”列表中再选择“修改”“写入”权限。

11.5　实战演练

实战演练1——检测网站的安全性



360网站安全检测平台为网站管理者提供了网站漏洞检测、网站挂马实时监控、网站篡改实时监控等服务。

使用360网站安全检测平台检测网站安全的操作步骤如下。

Step 01 在IE浏览器中输入360网站安全检测平台的网址http://webscan.360.cn/，打开360网站安全的首页，在首页中输入要检测的网站地址，如下图所示。



Step 02 单击“检测一下”按钮，即可开始对网站进行安全检测，并给出检测的结果，如下图所示。



Step 03 如果检测出来网站存在安全漏洞，就会给出相应的评分，然后单击“我要更新安全得分”按钮，就会进入360网站安全修复界面，如下图所示，在对站长权限进行验证后，就可以修复网站安全漏洞了。



实战演练2——查看网站的流量

使用CNZZ数据专家可以查看网站流量，CNZZ数据专家是全球最大的中文网站统计分析平台，为各类网站提供免费、安全、稳定的流量统计系统与网站数据服务，帮助网站创造更大价值。

使用CNZZ数据专家查看网站流量的具体操作步骤如下。

Step 01 在IE浏览器中输入网址http://www.cnzz.com/，打开“CNZZ数据专家”网站的主页，如下图所示。



Step 02 单击“免费注册”按钮进行注册，进入创建用户界面，根据提示输入相关信息，如下图所示。



Step 03 注册信息输入完毕并通过验证后，即可注册成功，并进入“添加站点”界面，如下图所示。

添加站点

网站名称：

网站域名：　1　未在此处设定的域名流量将不予统计，支持模糊匹配

网站首页：http://

网站类型：请选择网站类型

网站地区：请选择地区

网站简介：

Step 04 在“添加站点”界面中输入相关信息，如下图所示。

网站名称：你好

网站域名：　1　mysite.com

网站首页：www.mysite.com

网站类型：娱乐类　聊天

网站地区：上海市　上海市

网站简介：

确认添加站点

Step 05 单击“确认添加站点”按钮，进入“站点设置”界面，如下图所示。

站点设置

站点资料
获取代码
排名列表
排除受访
排除来路
排除访客IP
查看密码
关闭统计
进入统计报表

为站点 你好(www.mysite.com) 获取统计代码

统计代码

请任选一种形式的代码，将其粘贴到您网站所有页面的</body>前，添加成功后立即开始

展开了解更多

文字形式

图片形式1

复制到剪贴板

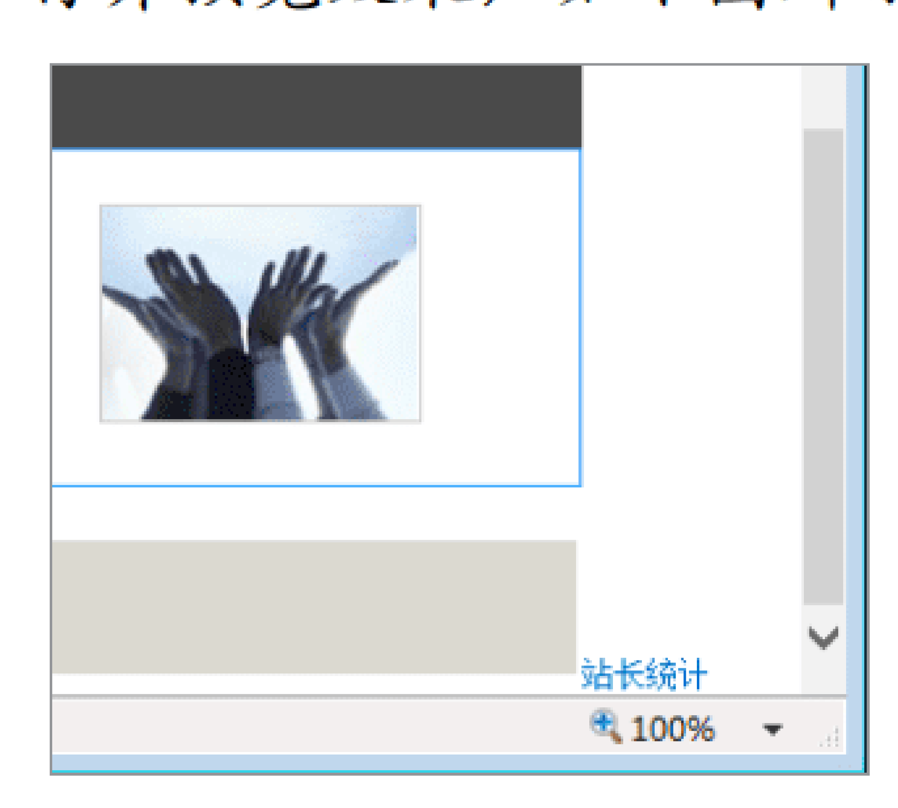
Step 06 在“统计代码”界面中单击“复制到剪切板”按钮，根据需要复制代码（此处选择“站长统计文字样式”），如下图所示。



Step 07 将代码插入到页面源码中，如下图所示。



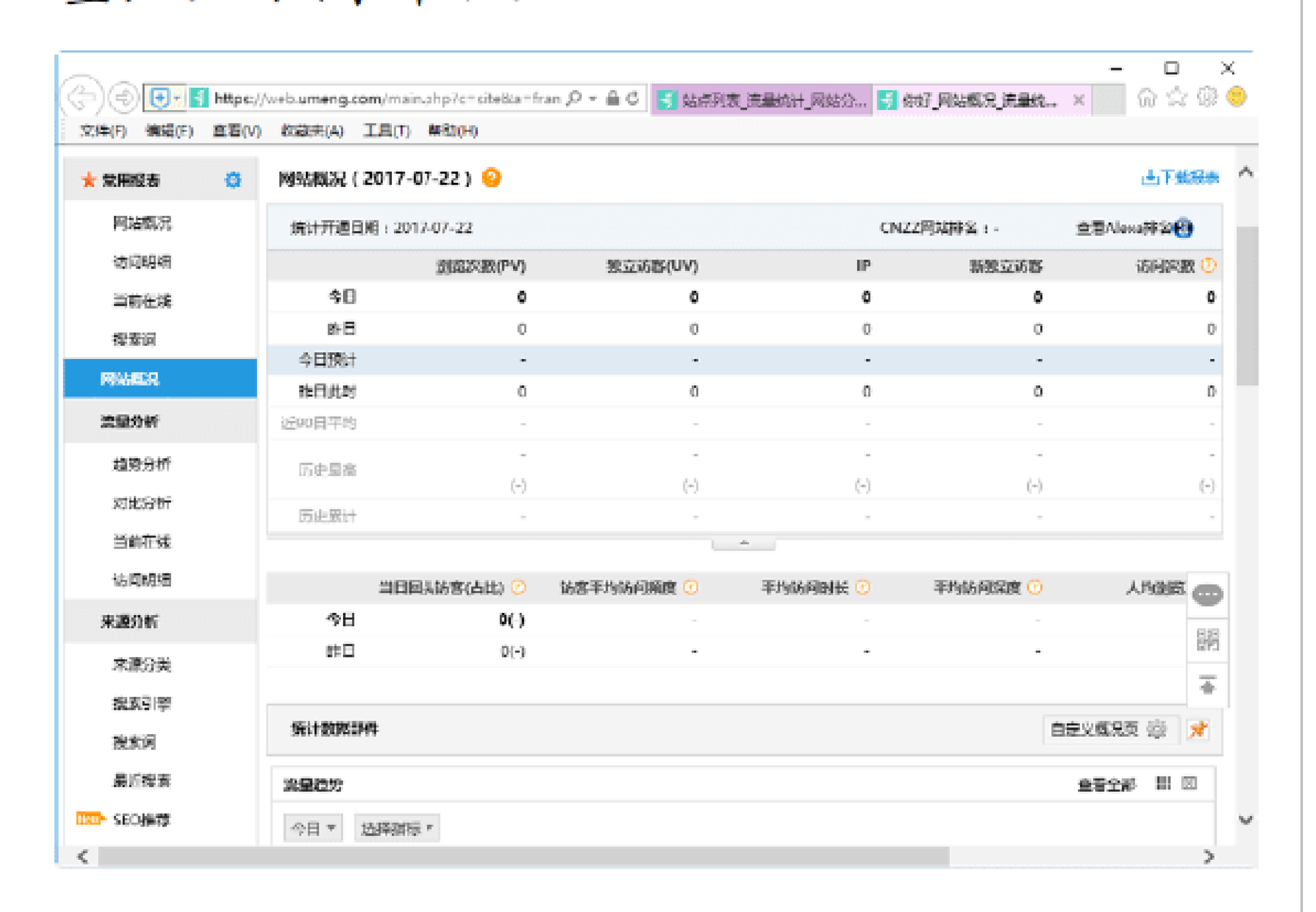
Step 08 保存并预览效果，如下图所示。



Step 09 单击“站长统计”按钮，进入“查看用户登录”界面，如下图所示。



Step 10 进入查看界面，即可查看网站的浏览量，如下图所示。



11.6 小试身手



练习1：添加网站的网址到收藏夹

Microsoft Edge浏览器的收藏夹其实就是一个文件夹，其中存放着用户喜爱或经常访问的网站地址，如果能好好利用这一功能，将会使网上冲浪更加轻松惬意。

将网页添加到收藏夹的具体操作步骤如下。

Step 01 打开一个需要将其添加到收藏夹的网页，如下图所示的新浪首页。



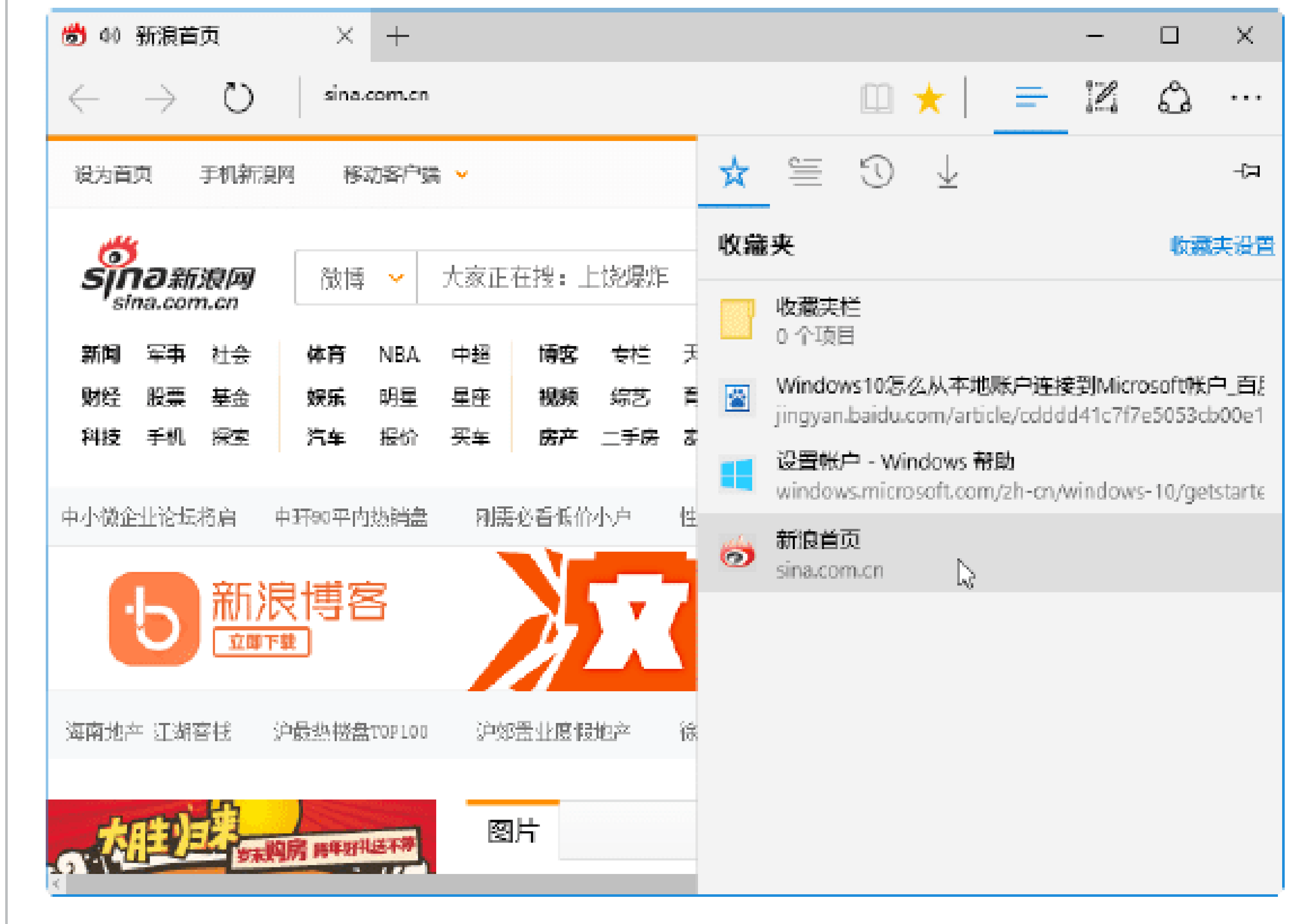
Step 02 单击页面中的“添加到收藏夹或阅读列表”按钮，如下图所示。



Step 03 打开“收藏夹或阅读列表”工作界面，在“名称”文本框中可以设置收藏网页的名称，在“保存位置”文本框中可以设置网页收藏时保存的位置，如下图所示。



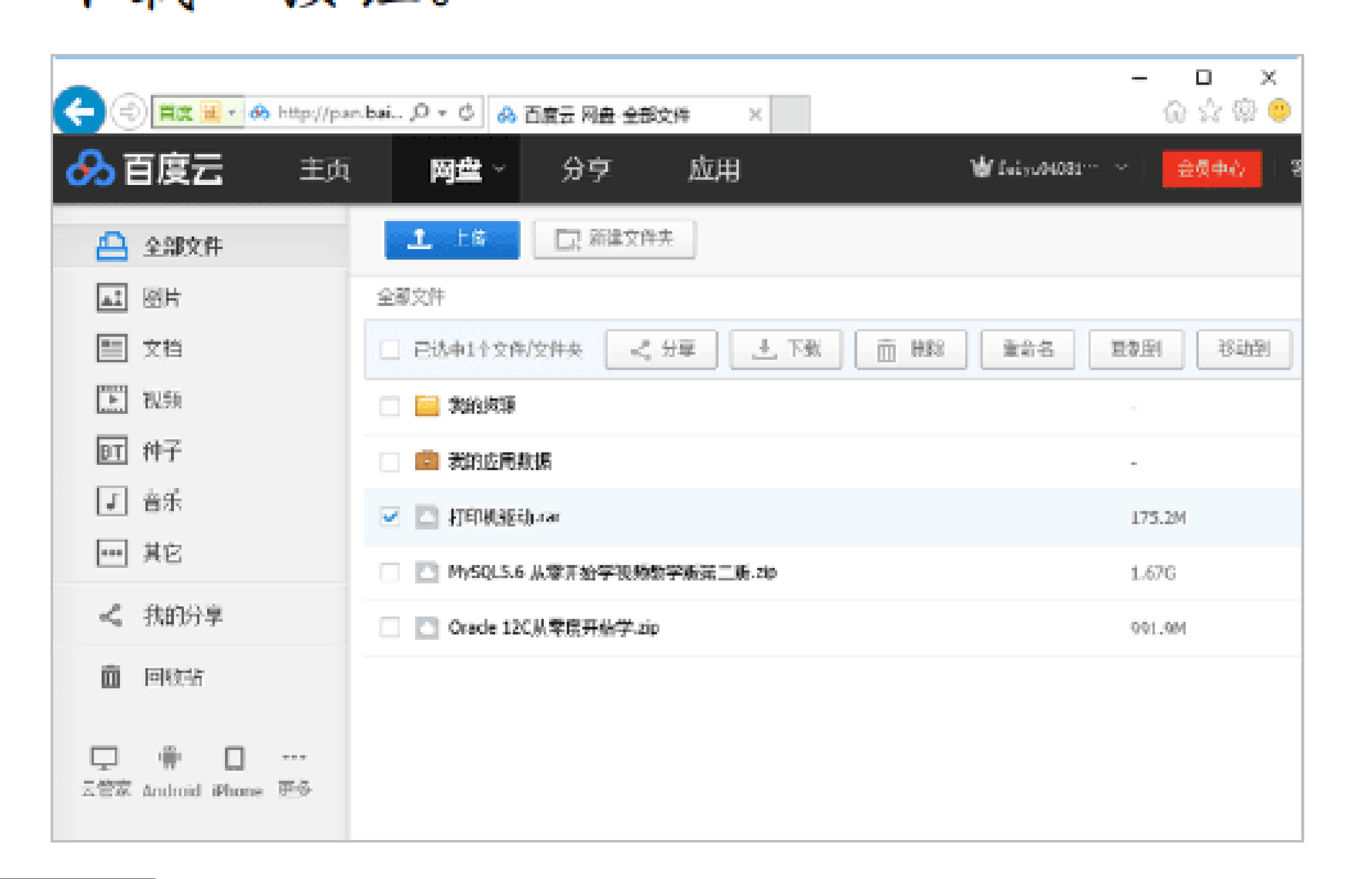
Step 04 单击“保存”按钮，即可将打开的网页收藏起来。单击页面中的“中心”按钮，打开“中心”设置界面，在其中单击“收藏夹”按钮，可以在下方的列表中查看收藏夹中已经收藏的网页信息，如下图所示。



练习2：下载网站中的资料资源

使用IE浏览器可以直接下载网站中的资料资源，下面以Internet Explorer 11浏览器为例，介绍在IE浏览器中直接下载文件的方法。一般网上的文件以.rar、.zip等扩展名存在。使用IE浏览器下载扩展名为.rar文件的具体操作步骤如下。

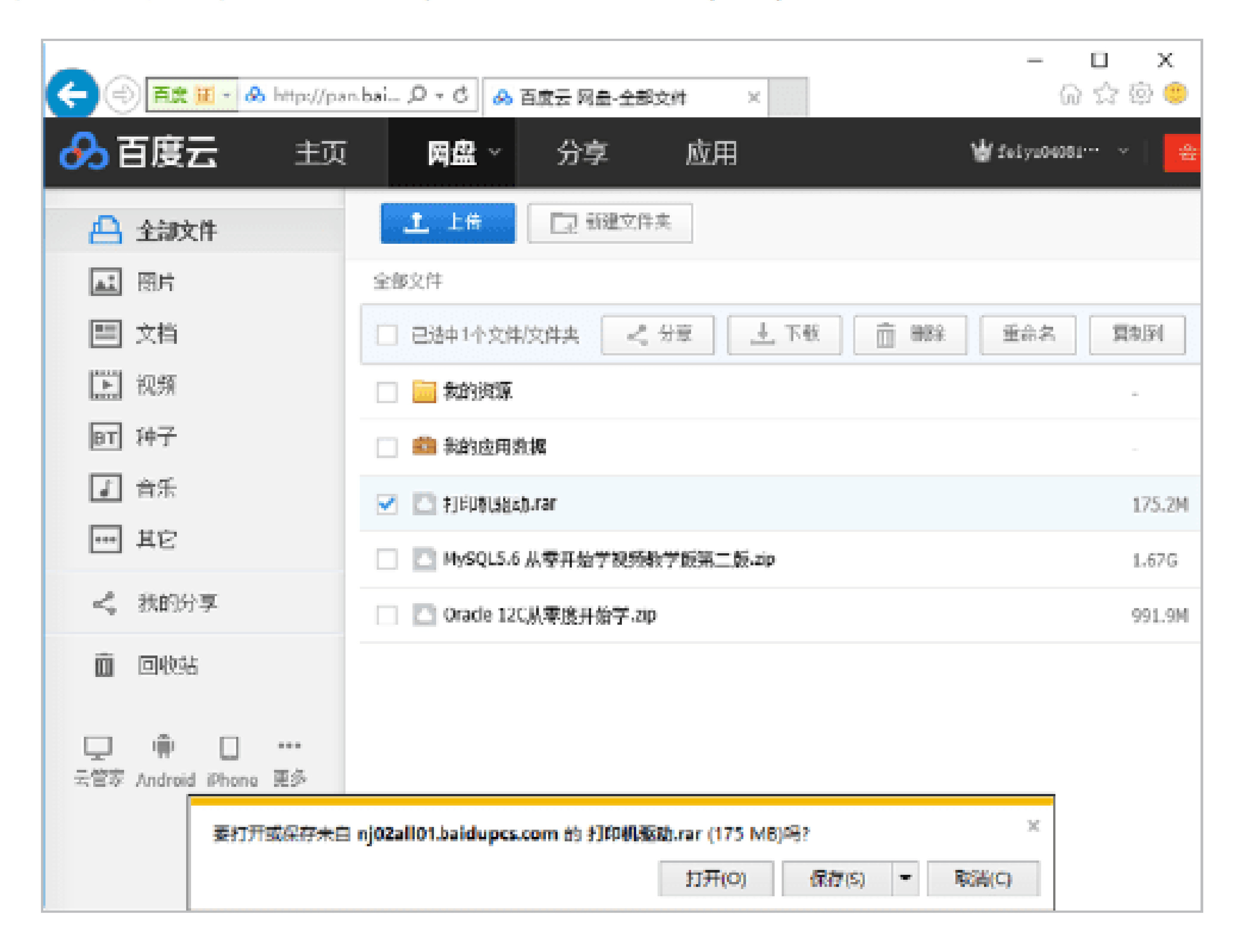
Step 01 这里以在百度云网盘中下载资料为例，打开要下载的文件所在的网站网页。单击需要下载的链接，如下图所示单击“下载”按钮。



Step 02 打开“文件下载”对话框，如下图所示。

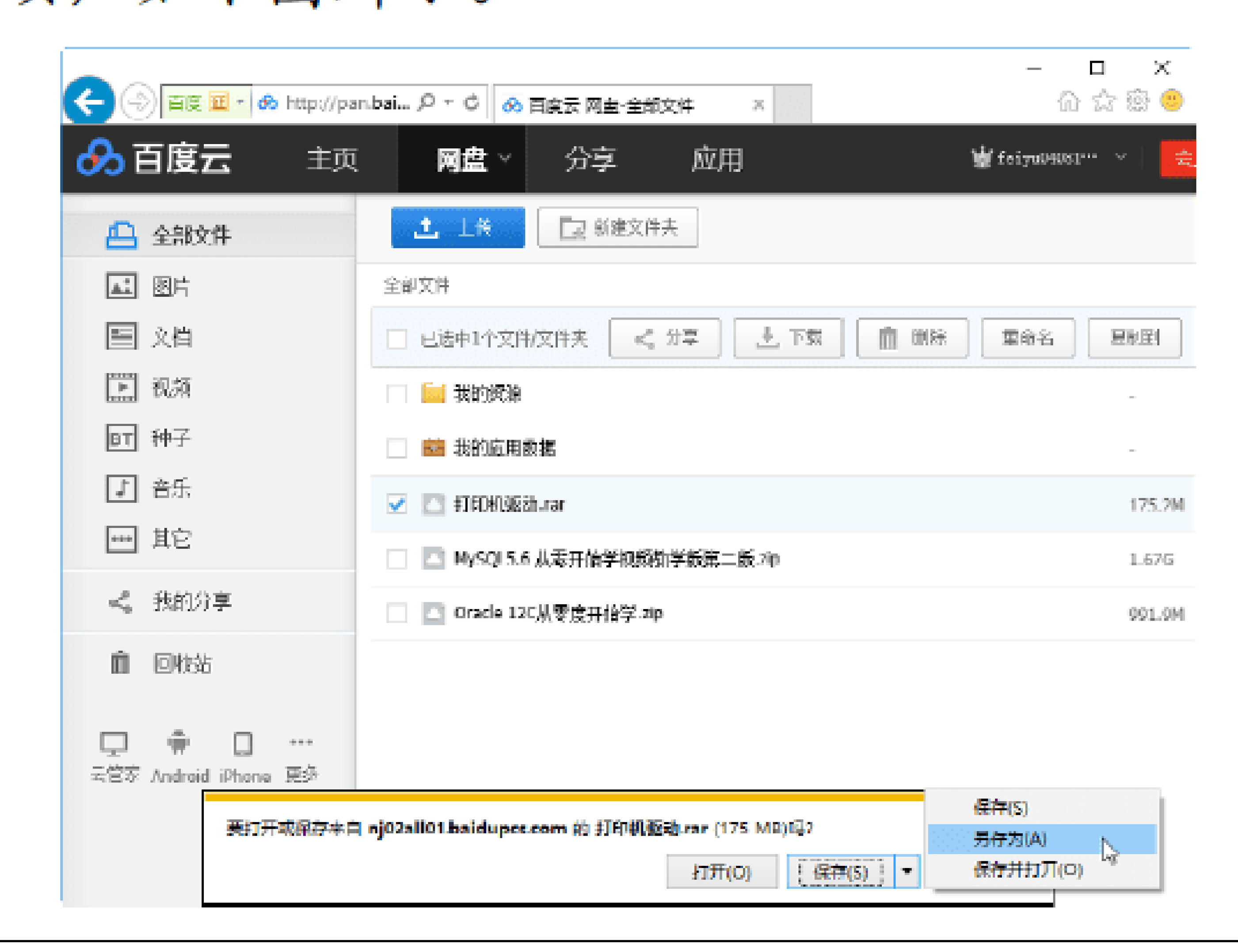


Step 03 单击“普通下载”按钮，在页面的下方显示下载信息提示框，提示用户是否运行或保存此文件，如下图所示。



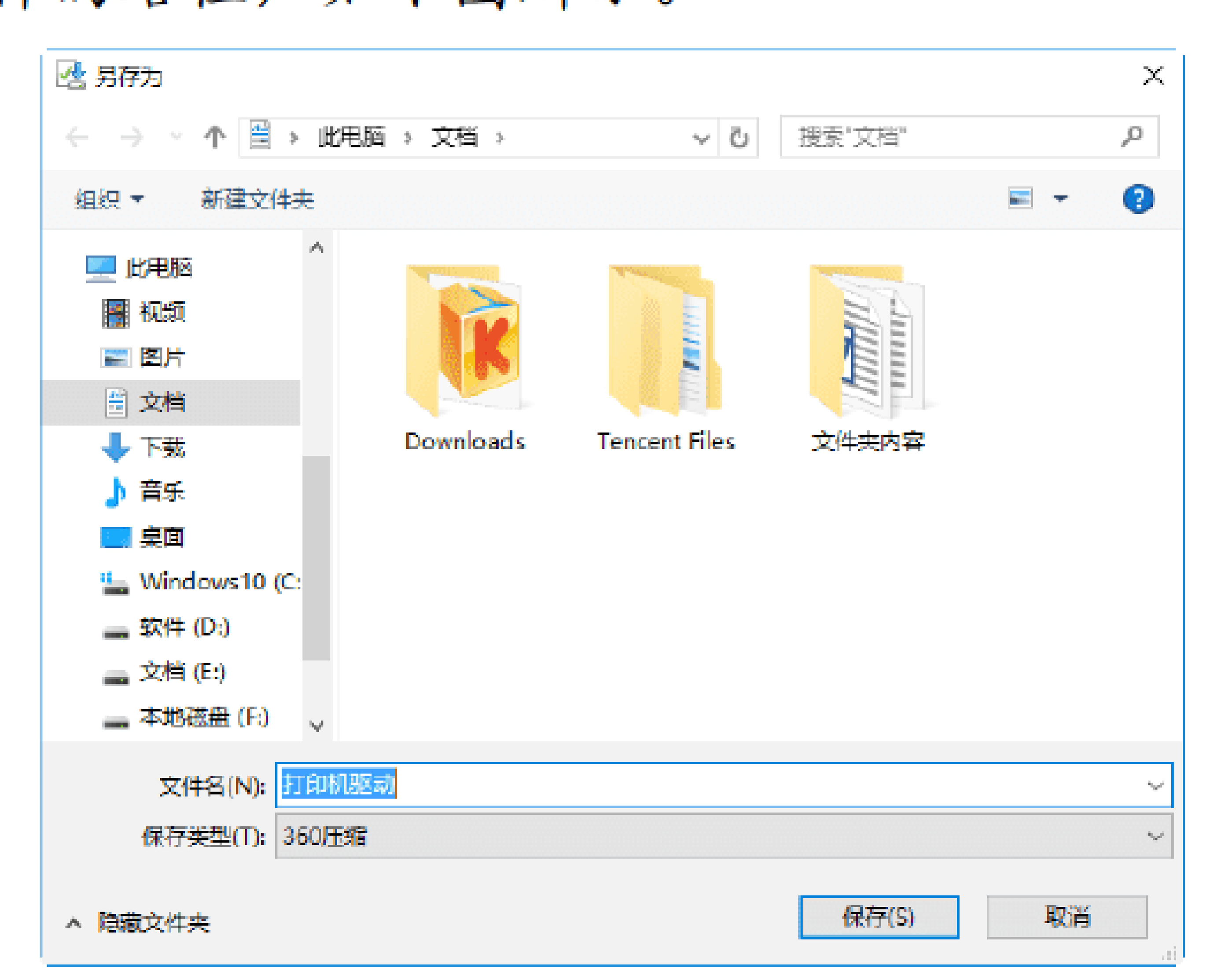


Step 04 单击“保存”按钮右侧的下拉按钮，在弹出的下拉列表中选择“另存为”选项，如下图所示。

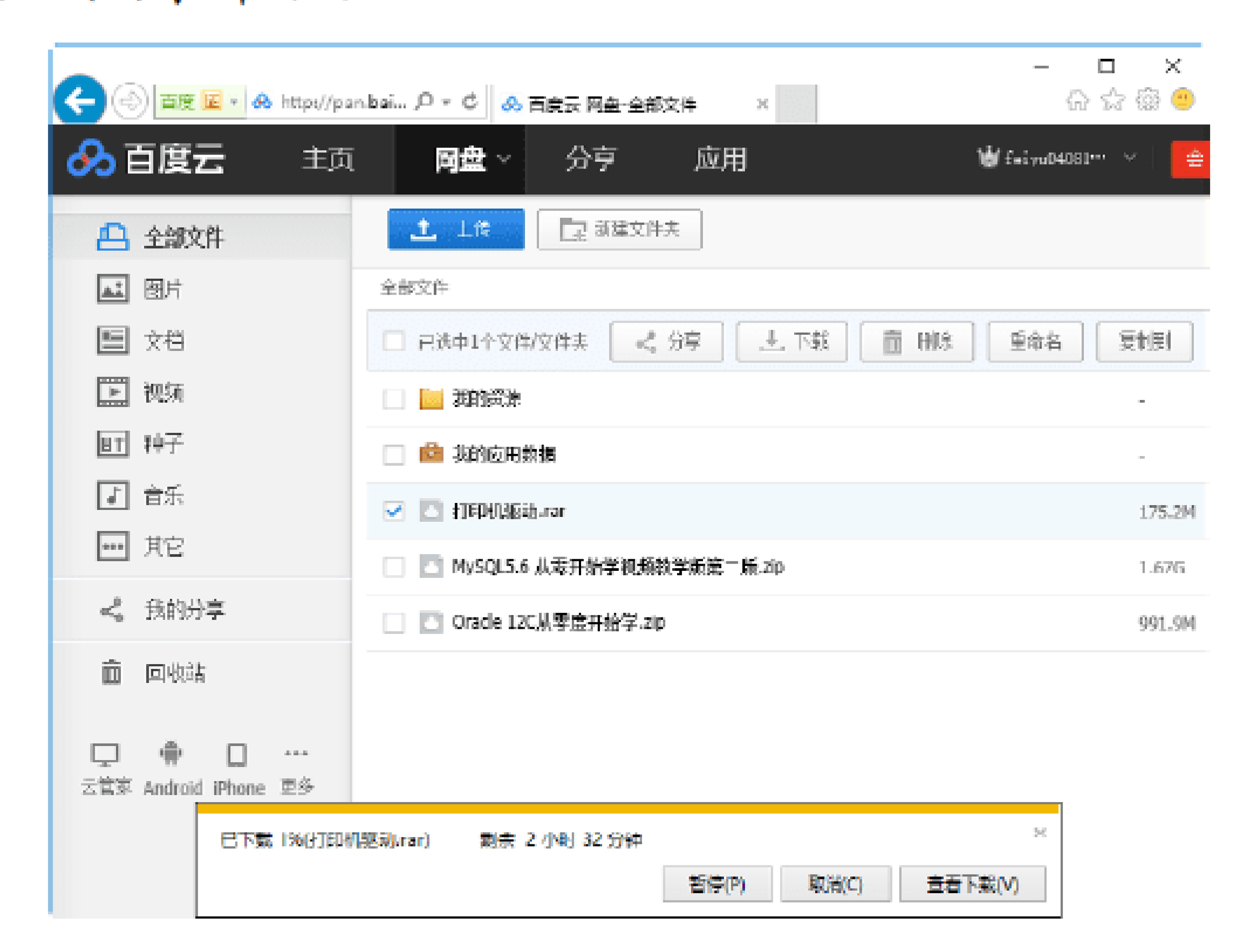


提示：在单击网页上的链接时，会根据链接的不同而执行不同的操作，如果单击的链接指向的是一个网页，则会打开该网页，当链接为一个文件时，才会打开“文件下载”对话框。

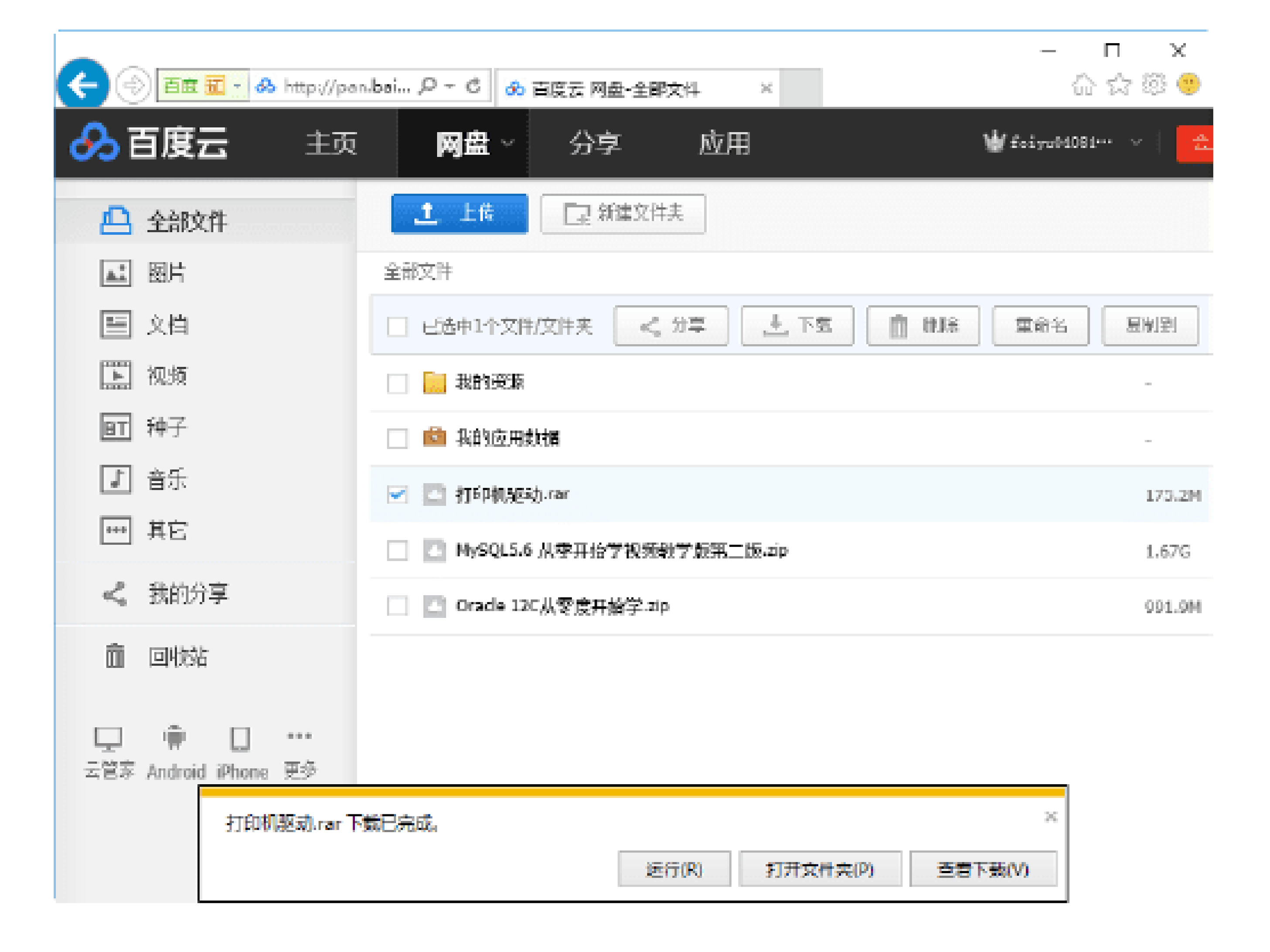
Step 05 打开“另存为”对话框，选择保存文件的路径，如下图所示。



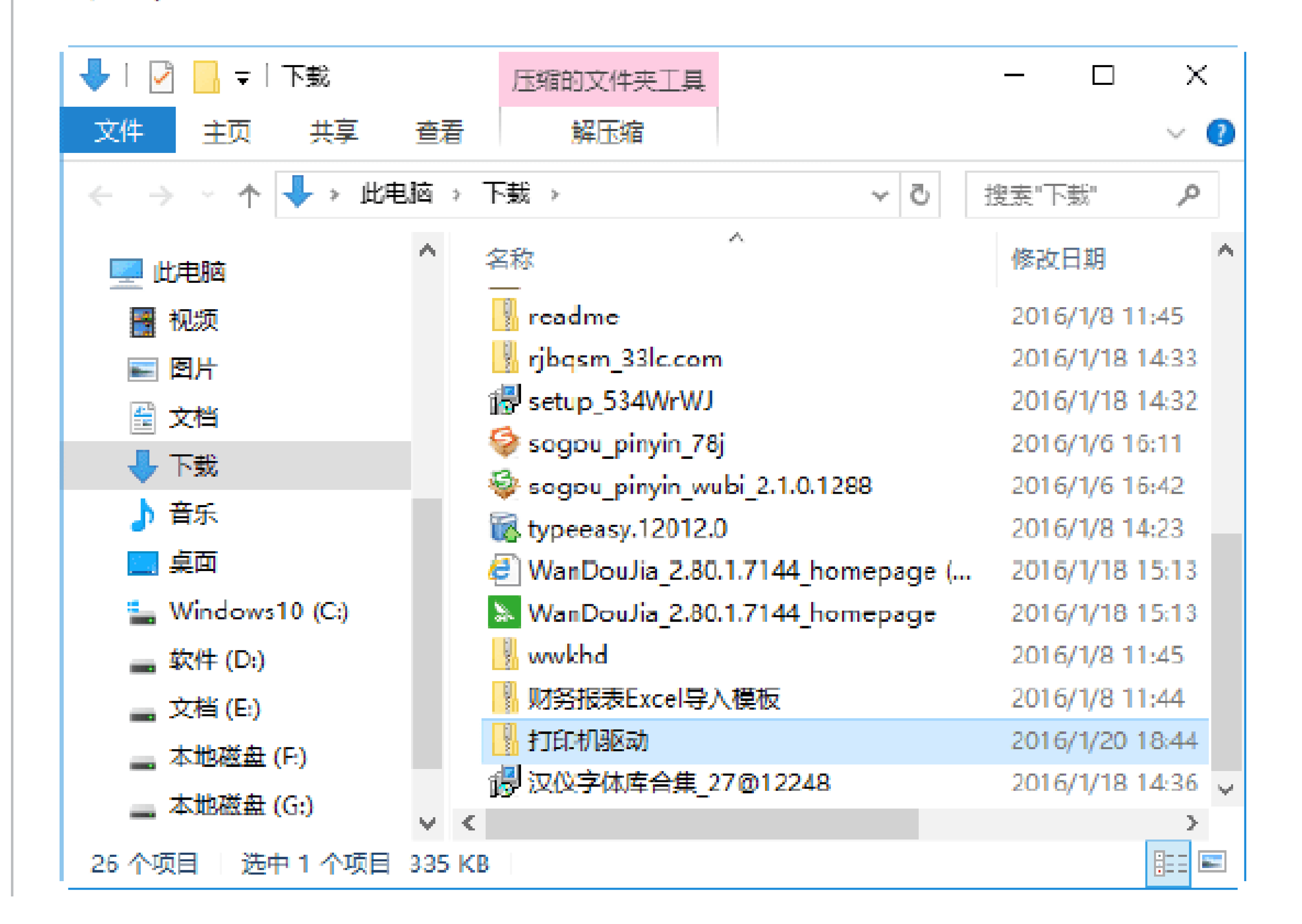
Step 06 单击“保存”按钮，开始下载文件，如下图所示。



Step 07 下载完成后，出现“下载已完成”提示框，如下图所示。



Step 08 单击“打开文件夹”按钮，可以打开下载文件所在的路径，如下图所示。单击“运行”按钮，即可执行程序的安装操作。



第12章　电子邮箱与邮件的安全防护

随着计算机与网络的快速普及，电子邮件作为便捷的传输工具，在信息交流中发挥着重要的作用。很多大中型企业和个人已实现了无纸办公，所有的信息都以电子邮件的形式传送，其中包括很多商业信息、工业机密和个人隐私。因此，电子邮件的安全性成为人们需要重点考虑的问题。

12.1　认识电子邮件病毒

电子邮件本身不会产生病毒，只是病毒的寄生场所。电子邮件病毒是指通过电子邮件传播的病毒，一般是夹在邮件的附件中，在用户运行附件中的病毒程序后，就会使计算机染毒。

12.1.1　电子邮件病毒的特征

电子邮件病毒其实和普通的计算机病毒一样，只不过由于它们的传播途径主要是通过电子邮件，也被称为“邮件病毒”。电子邮件病毒通常是把自己作为附件发送给被攻击者，如果接收到该邮件的用户不小心打开了附件，病毒即会感染用户的计算机。

现在大多数电子邮件病毒都会在感染用户的计算机之后自动打开Outlook中的地址簿，然后把病毒自身发送给地址簿上的每一个电子邮箱中，这正是电子邮件病毒能够一下子大面积传播的原因所在。另外，电子邮件客户端程序的一些Bug也可能被攻击者利用，传播电子邮件病毒。

“邮件病毒”除了具备普通病毒可传播性、可执行性、破坏性、可触发性特征之外，还具有以下几个特征：

（1）感染速度快。在单机环境下，病毒只能通过U盘或光盘等介质，从一台计算机传染到另一台。而在互联网中，绝大多数通过电子邮件传播的病毒都有自我复制和传播的能力，这正是它们的危险之处。它们不仅能够在用户发送邮件时把病毒自身进行复制传播，而且还能够主动选择用户邮箱地址簿中的地址发送带有病毒的邮件。根据测定，当网络正常使用情况下，只要有一台工作站有病毒，就可在几十分钟内将网上的数百台计算机全部感染。

（2）扩散面广。由于企业邮箱的邮件不仅仅在单个企业内部传播，还在互联网传送。这直接导致邮件病毒的扩散不仅快，而且扩散范围广，不但能迅速传染局域网内所有计算机，还能将病毒在一瞬间传播到千里之外。当其发作时，甚至可以造成整个网络的瘫痪，由此而造成的损失往往是难以估计的。

（3）清除病毒困难。单机上的计算机病毒有时可通过删除带毒文件、格式化硬盘等措施将病毒彻底清除。而企业中的计算机一旦感染了病毒，清除病毒变得非常困难，刚刚完成清除工作的计算机又有可能被网络中另一台带毒工作站所感染，使得清除邮件病毒变得非常困难。

（4）破坏性大。网络中的计算机感染了邮件病毒之后，将直接影响网络的工作。轻则降低速度，影响工作效率；重则使网络及计算机崩溃，资料丢失。

（5）隐蔽性。邮件病毒与其他病毒相比，更加隐蔽。一般来说，邮件病毒通常是隐蔽在邮件的附件中，或是邮件的信纸模板中，这一定程度上会加速病毒的泛滥，也增加了查杀病毒的难度。

12.1.2 识别电子邮件病毒

要想防范“邮件病毒”，必须能够准确地对其进行识别。下面将介绍3个识别“邮件病毒”的技巧。

（1）查看附件大小。电子邮件的附件通常是“邮件病毒”的最佳载体，通常查看附件大小，就可以识别电子邮件是否携带病毒。如果发现电子邮件的附件大小异常，则该封邮件有可能携带病毒。

（2）查看邮件地址。“邮件病毒”的传播者通常利用一些陌生的邮件地址发送邮件，当收到陌生的地址的邮件时，一定加倍小心。如果这类邮件有附件，更要谨慎，因为其极有可能携带病毒。对于陌生的邮件，在浏览了邮件地址后，再浏览邮件内容，无关痛痒且与工作无关，基本可以判定该邮件携带病毒。

（3）识别真伪退信。用户书写邮件时，如果将收件人的邮件地址写错，邮件服务器会自动将该邮件退回。一些“邮件病毒”的传播病毒，因为退信中有一个附件，该附件书写着用户邮件正文。一旦用户打开假冒的邮件服务器退信，并且查看了附件，“邮件病毒”将会立刻感染用户的计算机。

12.2 获取电子邮箱密码的常用手段

电子邮箱中一般保存着个人或公司的重要资料，而黑客则通过盗取邮箱密码的方式来入侵用户的电子邮箱，从而进行窃取机密文件、设置安装邮箱炸弹、散布邮件病毒等操作。

实战1：盗取邮箱密码的常用方法

为了保护电子邮箱，防止密码被黑客盗取，就有必要了解黑客盗取邮箱密码的一些常用手段，主要有以下几种。

1. 各个击破法

现在普通用户可以选择的电子邮箱种类很多，如腾讯、网易、搜狐、hotmail等。这些网站的邮箱系统本身都有很好的安全保障措施。而网易和腾讯邮箱在保障邮箱安全方面都运用了SSL技术，因此黑客如果要破解邮箱密码，必须要先研究SSL技术，进而进行突破。

黑客破解这种邮箱的关键是在加密的数据包上切开一个切口，然后将编译好的数据源利用数据交换的方式嵌入到加密的数据源上，利用编译的数据结合要破解邮箱密码的账号，编译的程序会以自定最小与最大密码长度的数字、字母、符号组成字符串找到正确的邮箱密码。但是由于各种邮箱的加密技术不同，要具体到每款邮箱来分析，从而实现各个击破的目的。

2. TCP/IP法

TCP/IP主要作用是在主机建立一个虚拟连接，以实现高可靠性的数据包交换。其中，IP可以进行IP数据包的分割和组装，而TCP则负责数据到达目标后返回来的确认。

根据TCP/IP的工作原理，黑客可以通过目标计算机的端口或系统漏洞潜入到对方，运行程序ARP；然后阻断对方的TCP反馈确认，此时目标计算机会重发数据包，ARP将接收这个数据包并分析其中的信息。

3. 邮箱破解工具法

由于上面的两种方法涉及的技术较高，操作过程也比较复杂，所以对于“菜鸟”级别的黑客而言并不适用。现在比较方便简单的方法是使用邮箱破解工具，如黑雨、溯雪、流光等，这些软件具有安装方便快捷、使用程序简便易懂、界面清新、一目了然、使用方便等特点。

实战2：使用“流光”盗取邮箱密码

“流光”是一款绝好的FTP、POP3解密工具，在破解密码方面，它具有以下功能：

（1）加入了本地模式，在本机运行时不必安装Sensor。

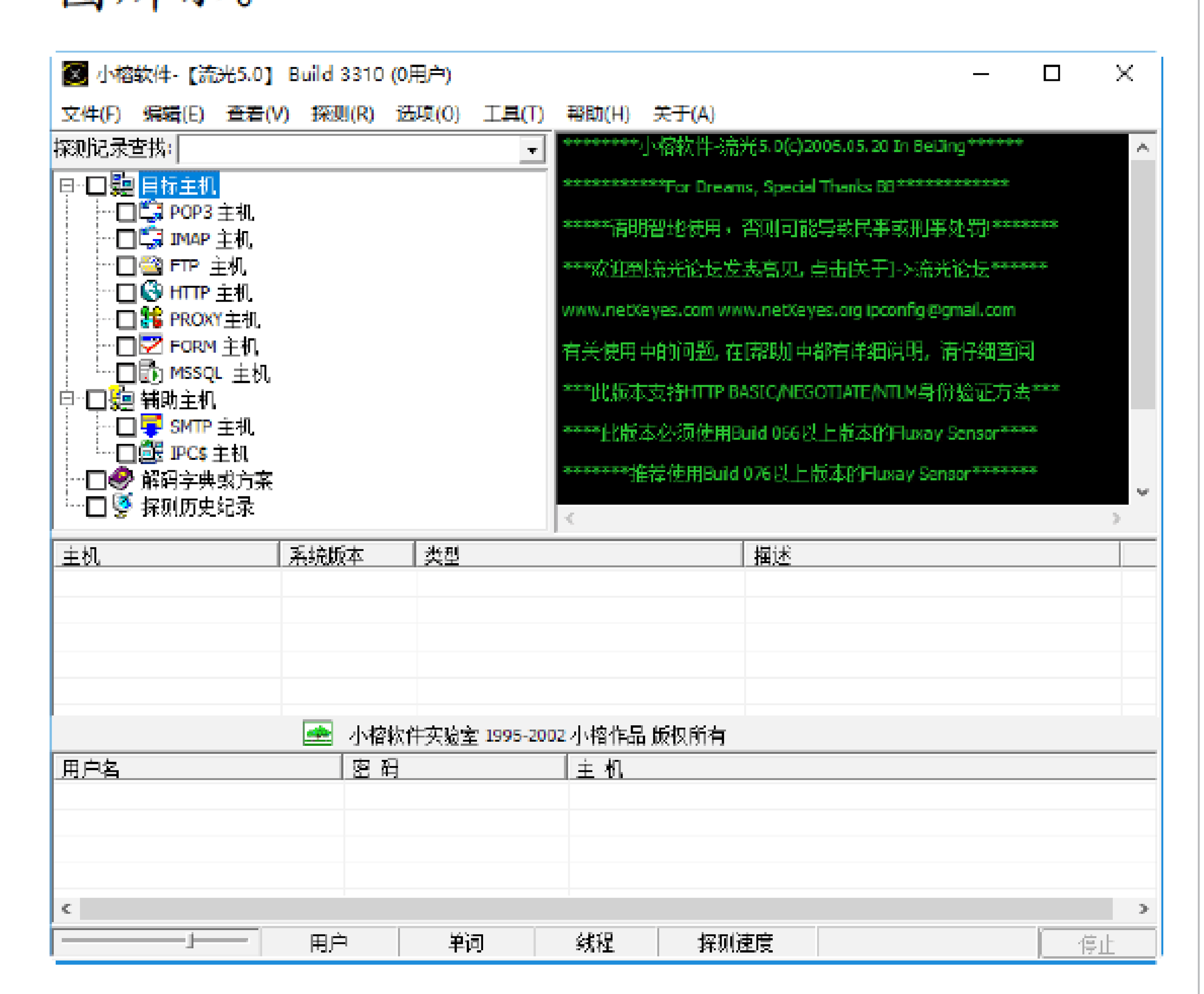
（2）用于检测POP3/FTP主机中用户密码安全漏洞。

（3）高效服务器流模式，可同时对多台POP3/FTP主机进行检测。

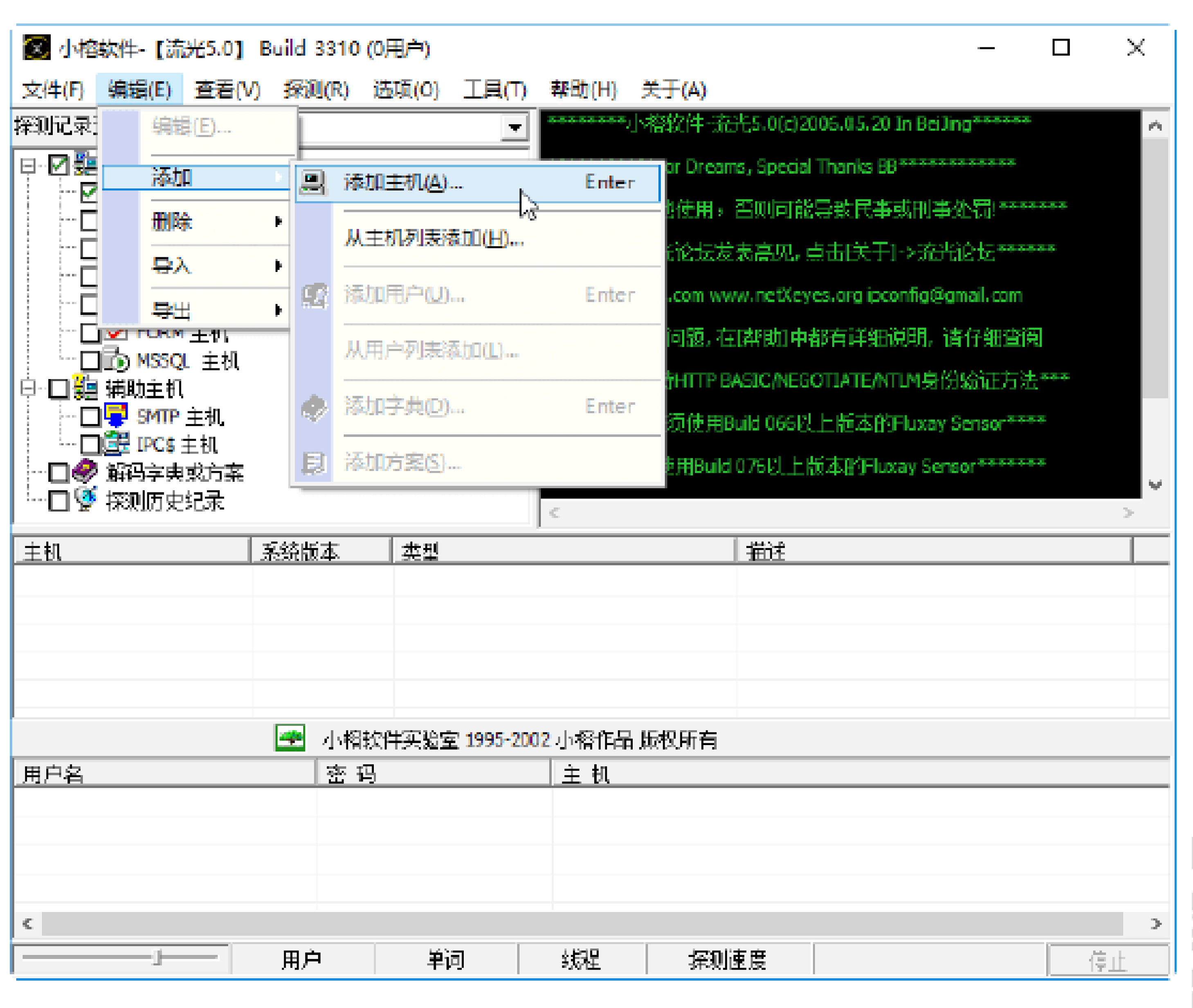
（4）支持10个字典同时检测，提高破解效率。

使用“流光”破解密码具体操作步骤如下。

Step 01 运行“流光”程序，主窗口显示如下图所示。



Step 02 勾选“POP3主机”复选框，选择“编辑”→“添加”→“添加主机”选项，如下图所示。

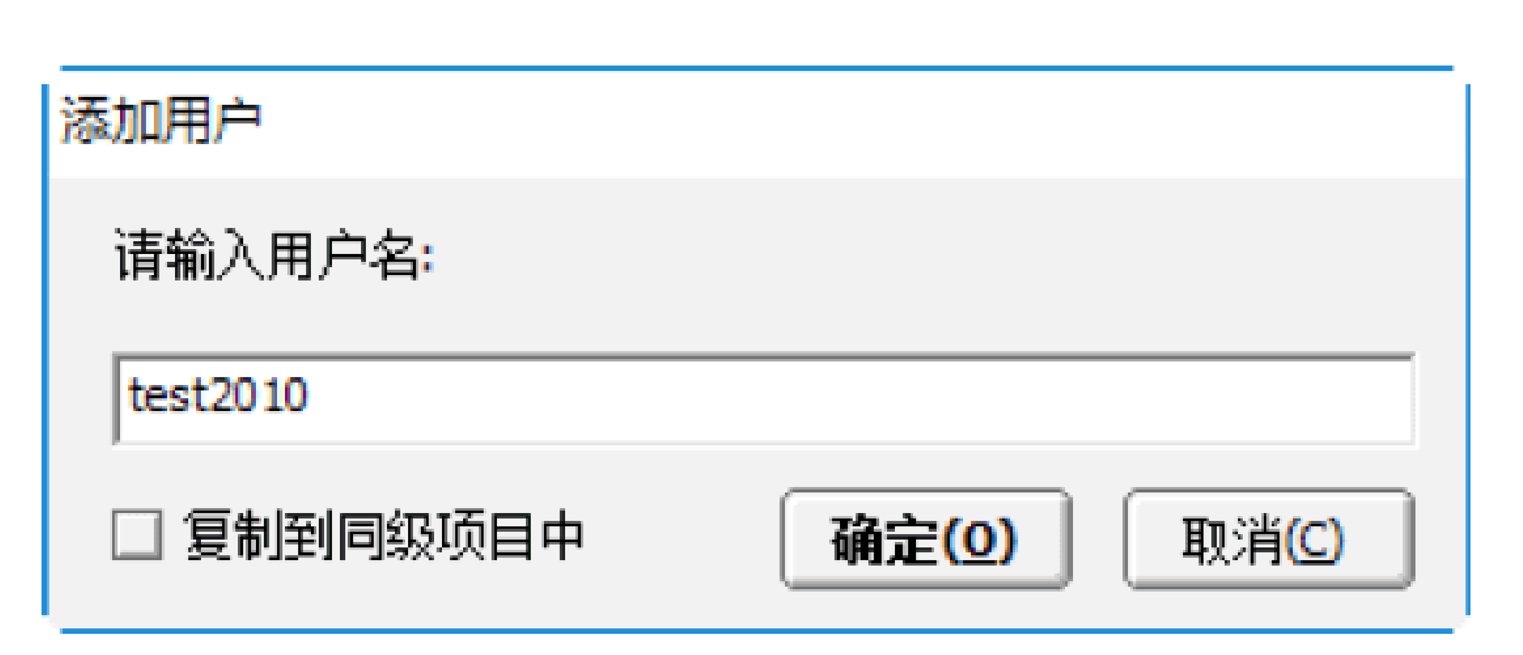




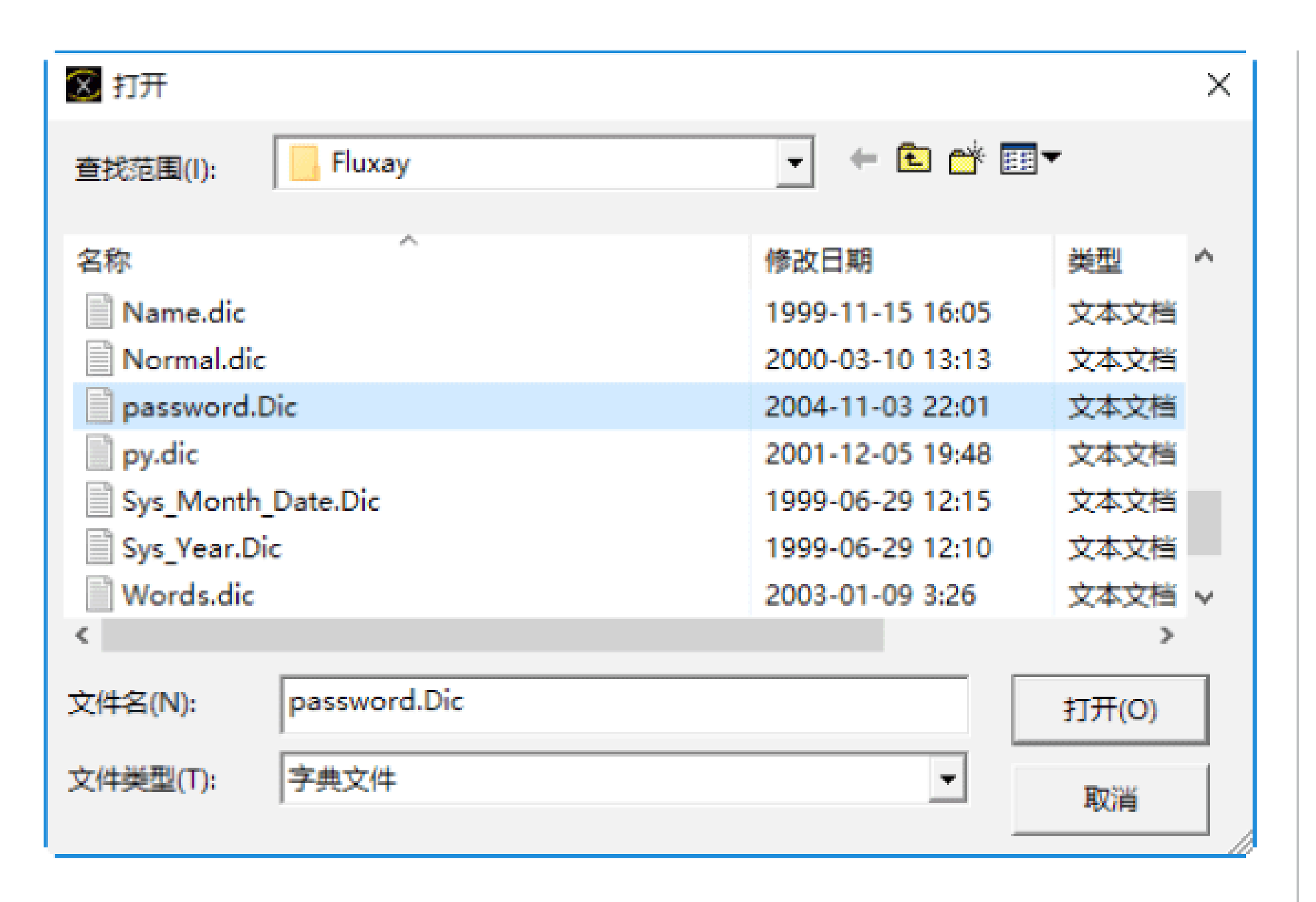
Step 03 打开“添加主机”对话框，在文本框输入要破解的POP3服务器地址，如下图所示，单击“确定”按钮。



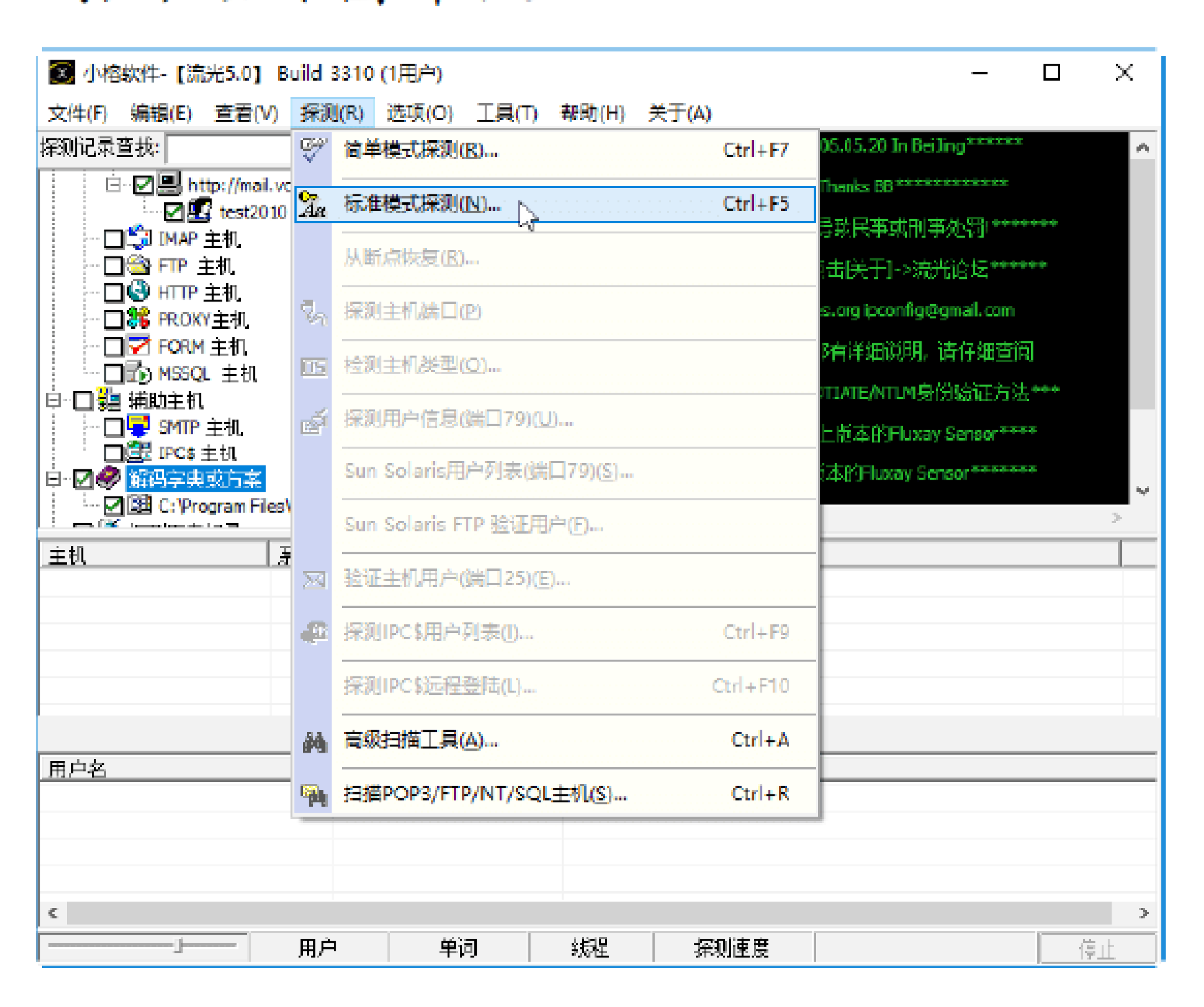
Step 04 勾选刚添加的服务器地址前的复选框，选择“编辑”→“添加”→“添加用户”选项，弹出“添加用户”对话框，在文本框中输入要破解的用户名，单击“确定”按钮，如下图所示。



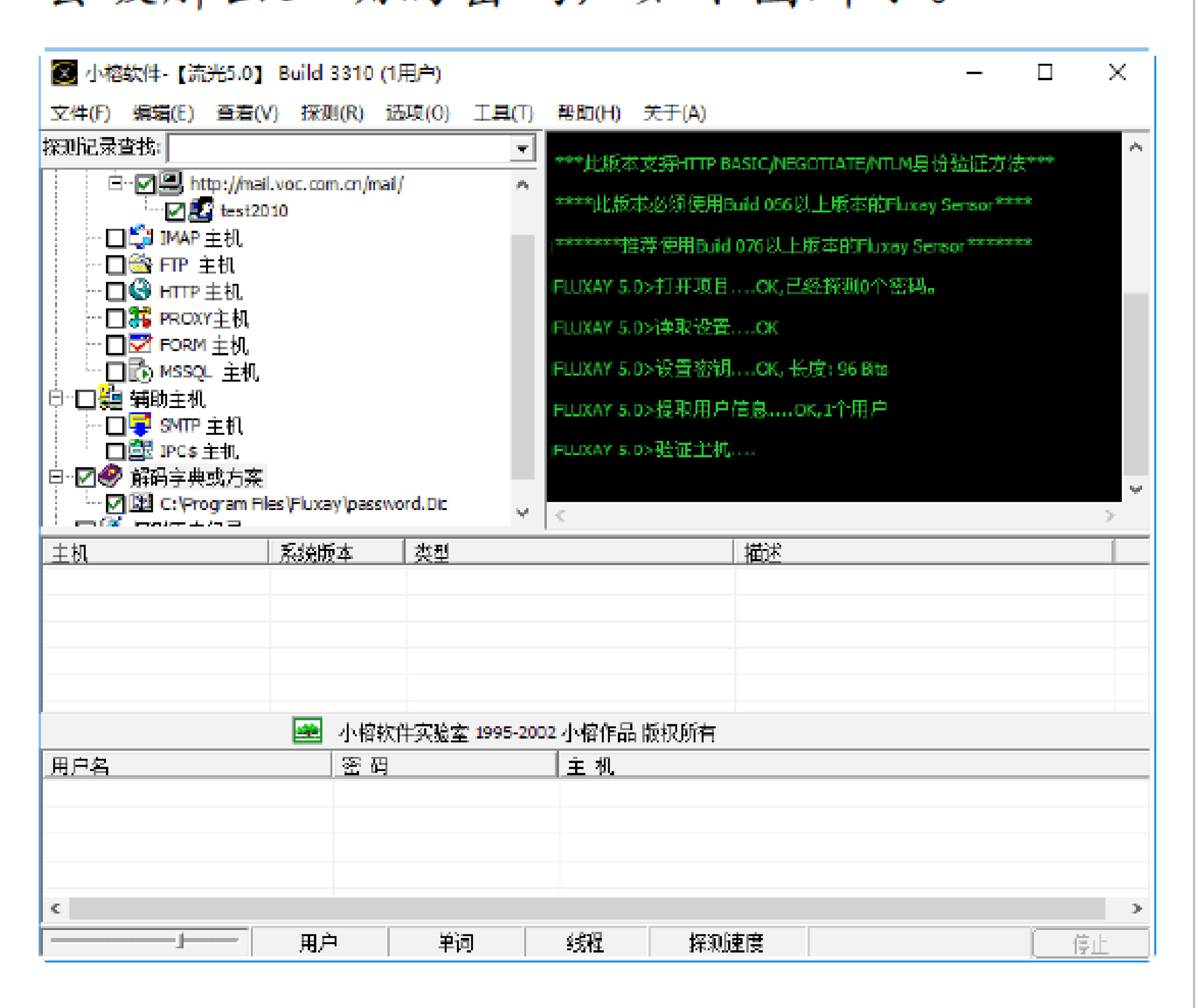
Step 05 勾选“解码字典或方案”复选框，选择“编辑”→“添加”→“添加字典”选项，弹出“打开”对话框，选择要添加的字典文件，单击“打开”按钮，如下图所示。



Step 06 选择“探测”→“标准模式探测”选项（“简单模式探测”功能不用指定具体的字典文件，使用流光内置的简单密码），如下图所示。



Step 07 “流光”开始进行探测，右窗格中显示实时探测过程。如果字典选择正确，就会破解出正确的密码，如下图所示。



12.3 电子邮箱与邮件的安全防护策略

电子邮箱是重要的网络交流工具，具有方便、快捷、实时的特点。在电子邮箱中，经常存放一些重要的信件和信息。一旦邮箱受到攻击，很可能泄露邮件中的重要信息，并可能导致网络瘫痪。因此，更应该重视保护邮箱安全。下面将详细介绍如何防范电子邮件攻击。

实战3：重要邮箱的保护措施

重要邮箱是用户用于存放比较重要的邮件和信息的邮箱，需要采取一些措施进行保护。

1. 使用备用邮箱

建议用户不要轻易把自己的重要邮箱地址泄露给他人，但在某些网站或BBS上，需要用户进行邮箱注册才能实现浏览和发帖等功能；或是在工作中需要用邮箱进行交流、发布信息等，这时就需要使用备用邮箱。

用户可以申请一个免费邮箱作为备用邮箱，利用这个邮箱订阅新闻、电子杂志，放在自己的个人主页上，在自己感兴趣的论坛或者BBS上使用，或是用于代表公司对外进行业务联系。

需要注意的是，如果是利用了备用邮箱进行过一些必要的网络服务申请，应该把确认信息再转发到自己的私人邮箱中备用。

2. 保护邮箱密码

除了要保护好重要邮箱的地址以外，邮箱的密码也是需要重点保护的，主要可以采取以下几种方式来防止攻击者进行暴力破解。

（1）密码选择。密码至少要有8位，并且密码里要包括至少一个数字、一个大写字母和一个小写字母，最好能包括一个符号。这种字母、数字和符号组成的密码，对于暴力破解软件来说，是比较不易被破解的。另外，密码最好不要包括用户的名字缩写、生日、手机号、公司电话等公开信息。

（2）定期更改密码。要养成定期更改密码的习惯，最好每一个月更改一次密码，这样会大大增加破解密码的难度。

（3）启用邮箱密码保护功能。通过设置密码保护，可以在忘记密码时通过回答密码提示问题或发送短信验证的方式取回密码。

实战4：找回被盗的邮箱密码

如果邮箱密码已经被黑客窃取甚至篡改，此时用户应该尽快将密码找回并修改密码，以避免重要的资料丢失。目前，绝大部分的邮箱都提供恢复密码功能，用该功能找回邮箱密码，以便邮箱服务的继续使用。

下面介绍找回163邮箱密码的具体操作步骤。

Step 01 首先在IE浏览器中打开163邮箱的登录页面（http://mail.163.com），如下图所示。



Step 02 单击“忘记密码了”超链接，打开“网易通行证”窗口，在其中即可看到各种修复密码的方法，如下图所示。



Step 03 单击“通过密码提示问题”超链接，打开“通过生日和密码提示问题”窗口，如下图所示。





Step 04 在其中输入申请邮箱时设置的问题的答案后，单击“下一步”按钮，打开“重新设置密码”窗口，如下图所示。



Step 05 在输入新密码和验证码后，单击“下一步”按钮，即可看到“您已成功设置您的网易通行证密码”提示框，如下图所示，单击“登录”超链接，即可直接登录自己的邮箱。

提示信息

恭喜您：[redacted]，您已成功设置您的网易通行证密码！

我要--> 登录

实战5：通过邮箱设置防止垃圾邮件

在电子邮箱的使用过程中，遇到垃圾邮件是很稀松平常的事情，那么如何处理

这些垃圾邮件呢？用户可以通过邮箱设置防止垃圾邮件。下面以在QQ邮箱中设置防止垃圾邮件为例，介绍通过邮箱设置防止垃圾邮件的方法。具体的操作步骤如下。

Step 01 在QQ邮箱工作界面中单击“设置”超链接，进入“邮箱设置”页面，如下图所示。



Step 02 在“邮箱设置”页面中选择“反垃圾”选项，即可进入“反垃圾”设置页面，如下图所示。



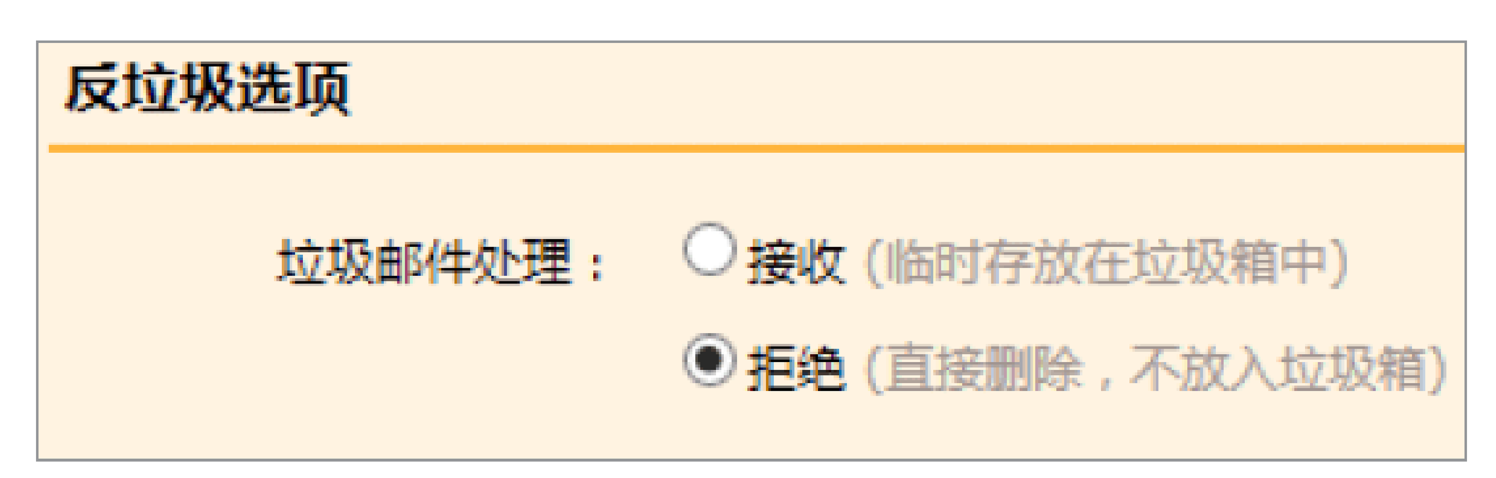
Step 03 单击“设置邮件地址黑名单”链接，进入“设置邮件地址黑名单”页面，在其中输入邮箱地址，如下图所示。



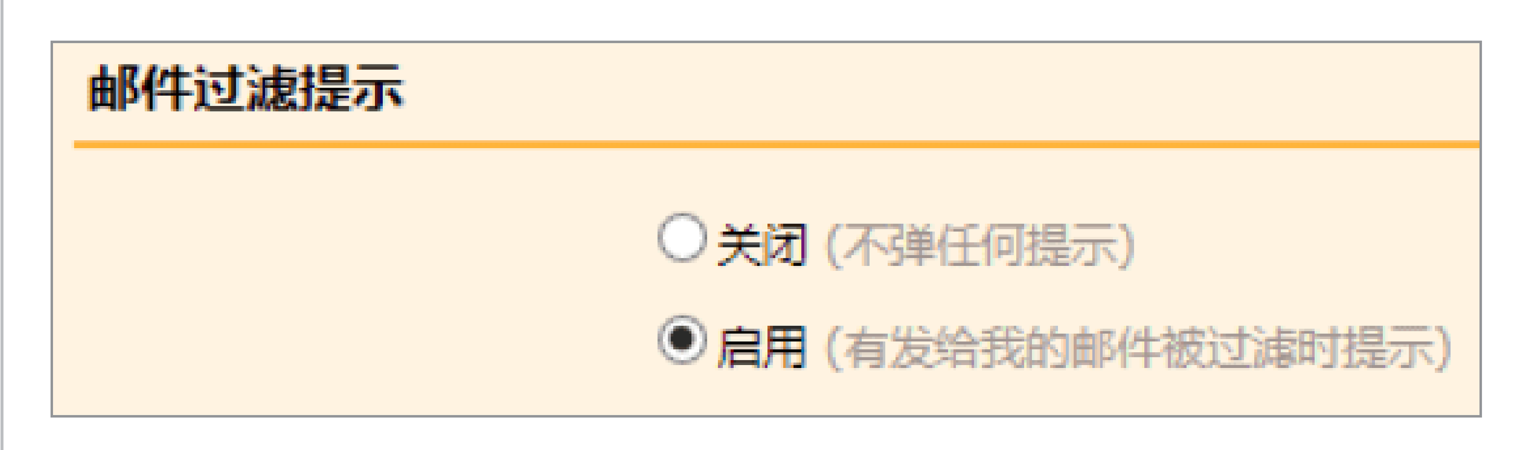
Step 04 单击“添加到黑名单”按钮，即可将该邮箱地址添加到黑名单列表中，如下图所示。



Step 05 单击“返回‘反垃圾’设置”超链接，进入“反垃圾选项”页面，在“反垃圾选项”页面中选中“拒绝”单选按钮，如下图所示。



Step 06 在“邮件过滤提示”页面中选中“启用”单选按钮，这样有发来的邮件被过滤时会给出相应的提示，如下图所示。



Step 07 设置完毕后，单击“保存更改”按钮，即可保存修改，如下图所示。



12.4　实战演练

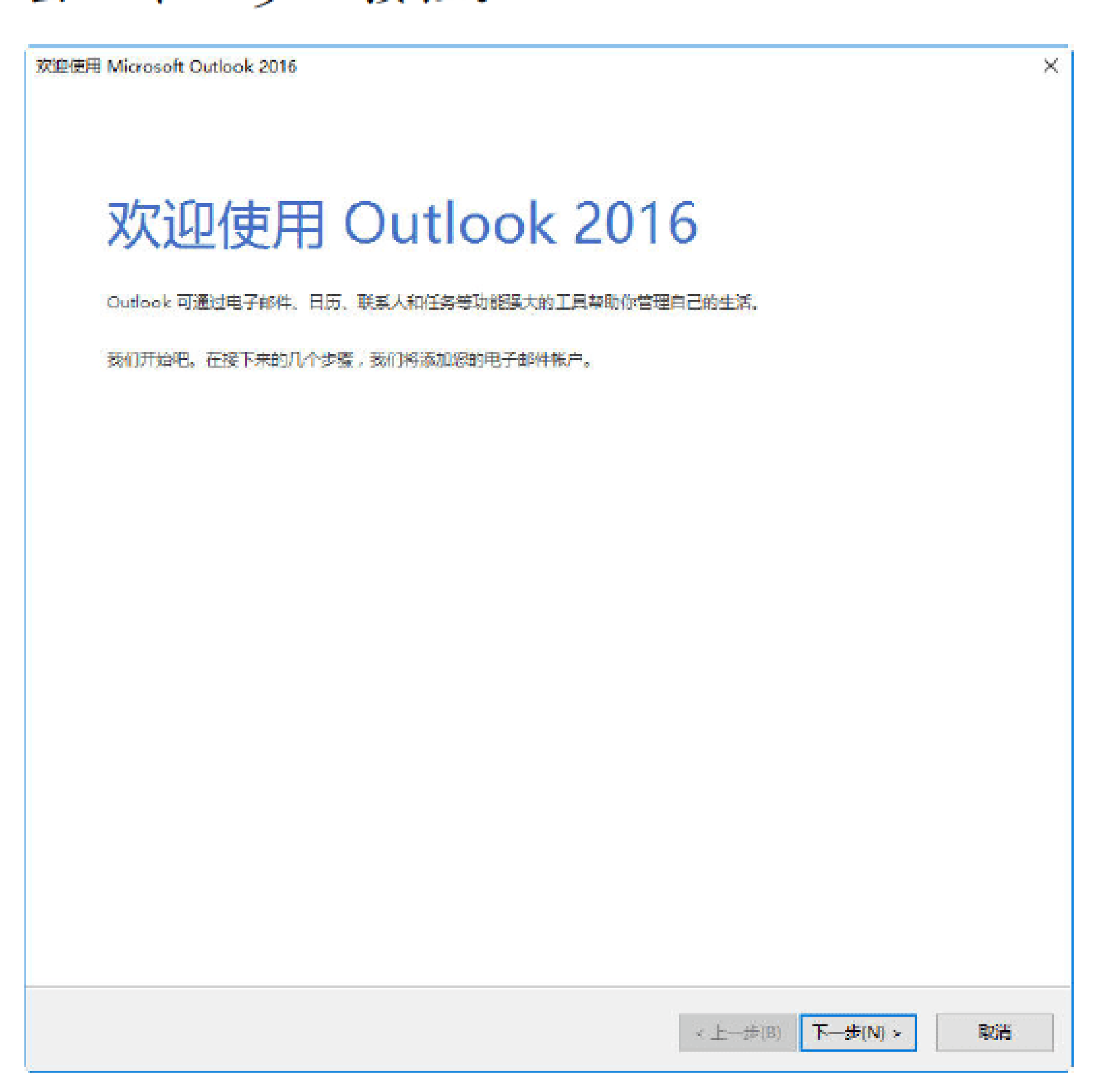
实战演练1——配置Outlook电子邮箱账户

首次使用Outlook 2016软件需要配置一个电子邮箱账户，配置邮件账户的具体操作步骤如下。

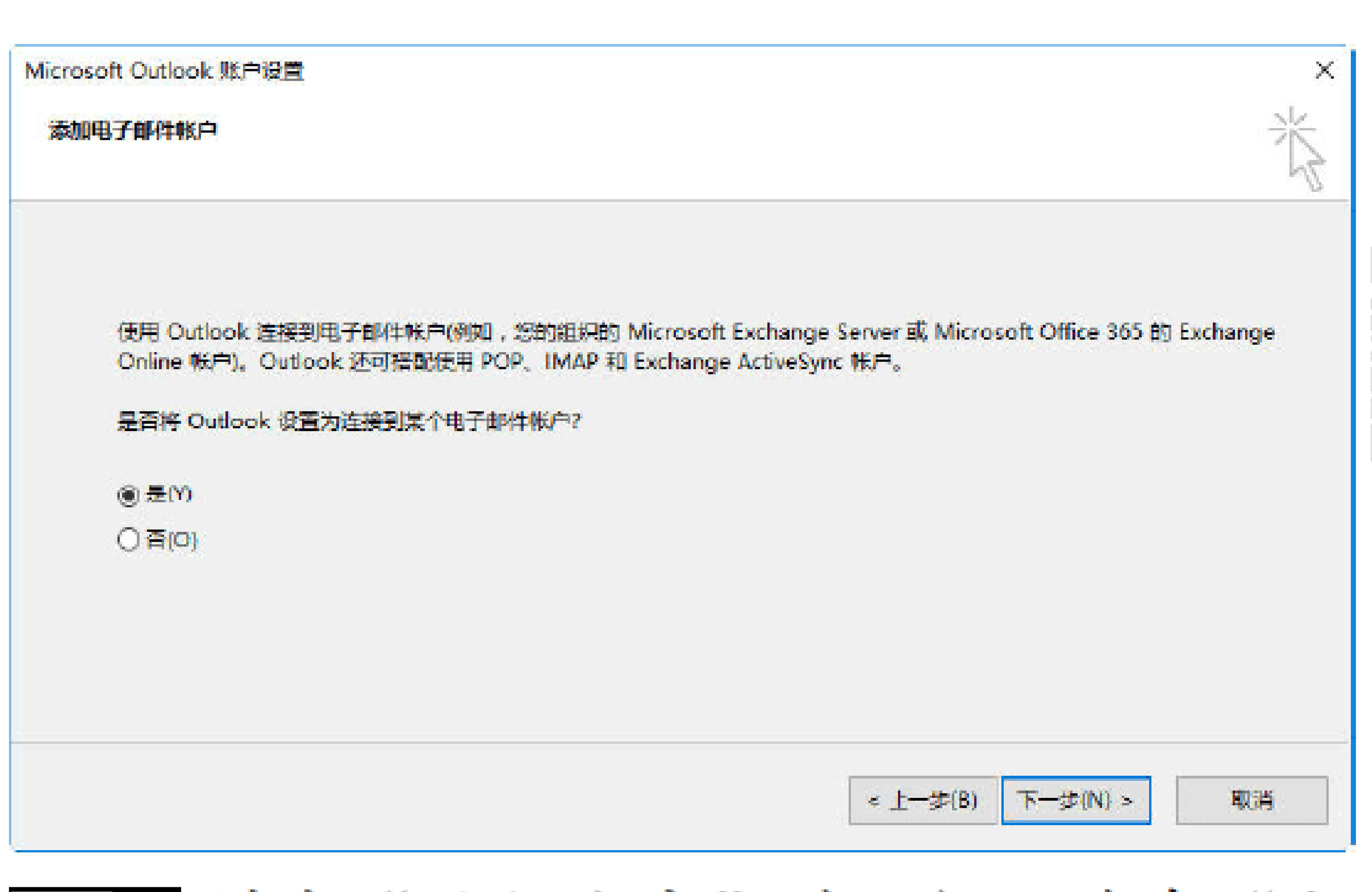
Step 01 在“开始”按钮，在弹出的程序列表中选择“所有应用”→“Outlook 2016”选项，如下图所示。



Step 02 弹出“欢迎使用Microsoft Outlook 2016”对话框，如下图所示，初次使用Outlook 2016需要配置Outlook账户，然后单击“下一步”按钮。

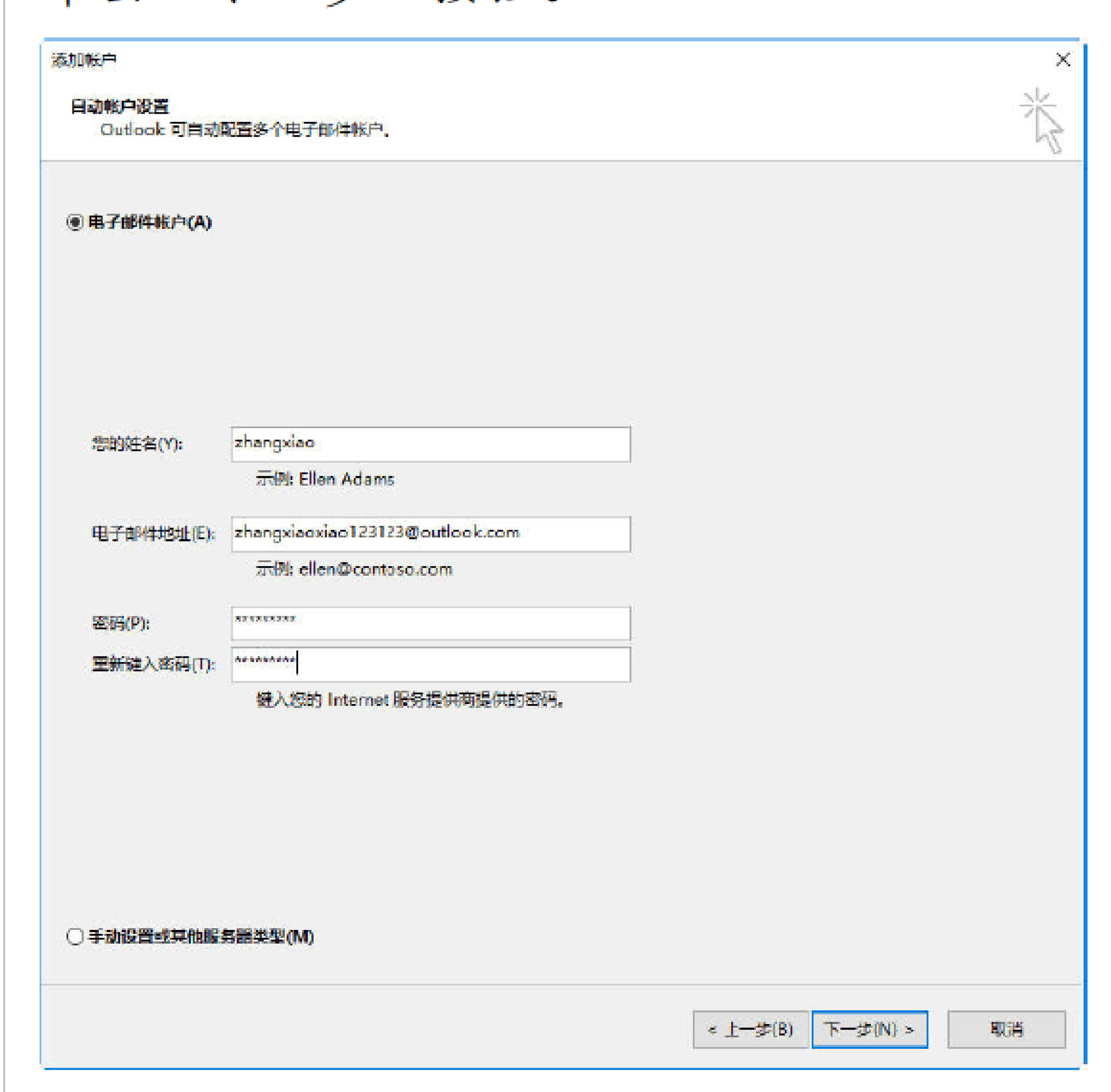


Step 03 弹出“Microsoft Outlook 账户配置”对话框，选中“是”单选按钮，如下图所示，单击“下一步”按钮。

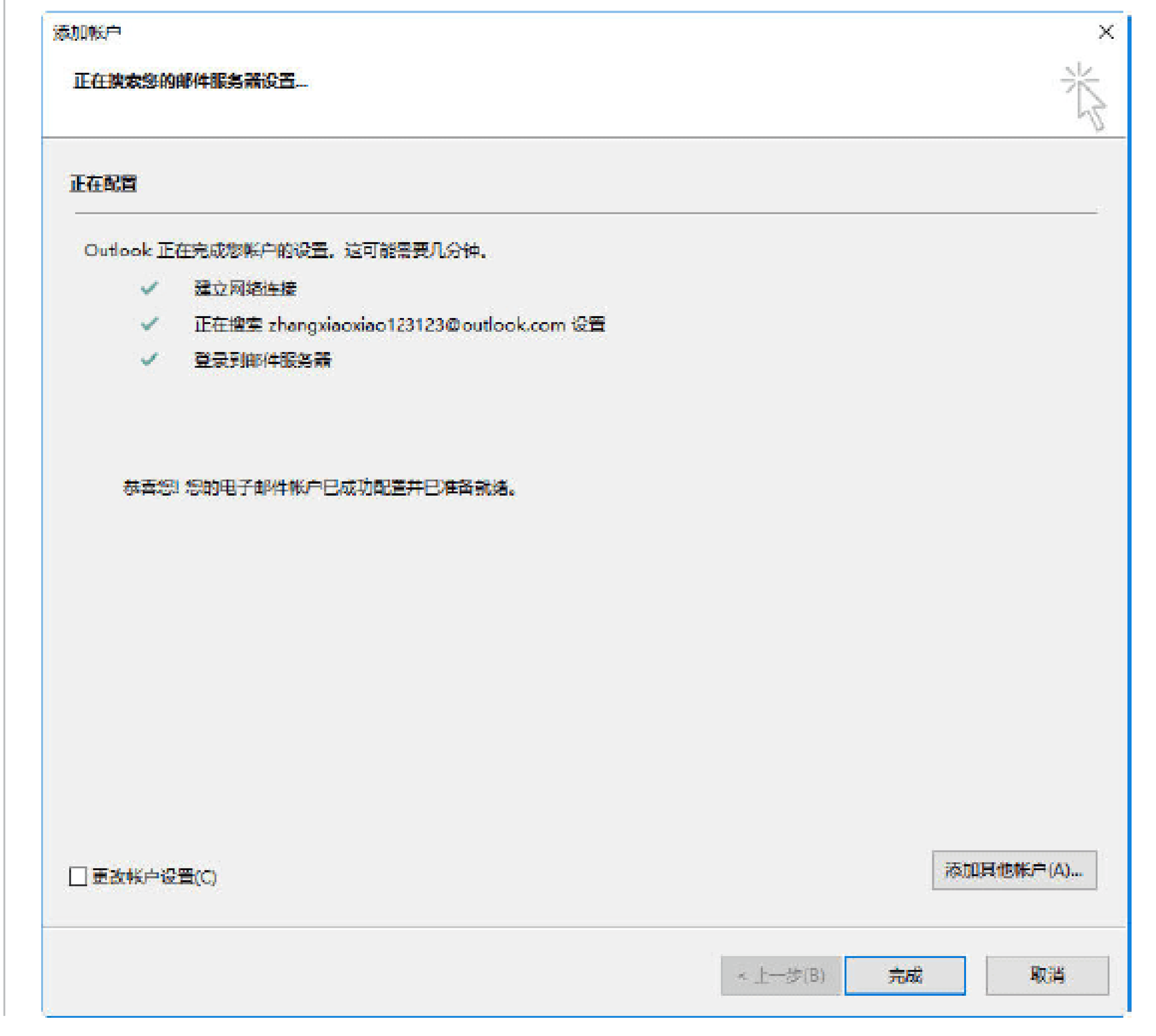




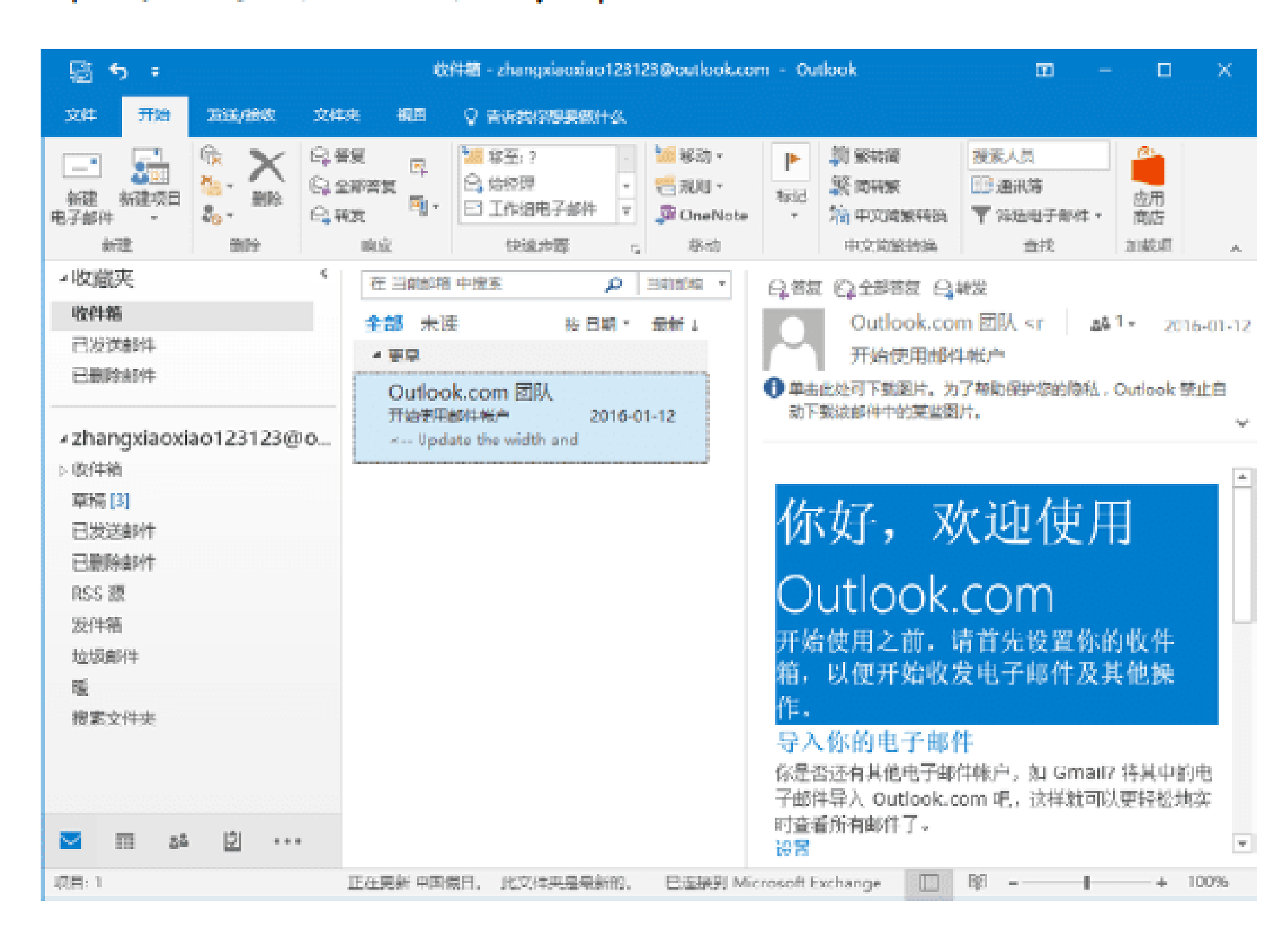
Step 04 弹出“添加账户”对话框，选中“电子邮箱账户”单选按钮，填写相关的姓名、电子邮件地址等信息，如下图所示，单击“下一步”按钮。



Step 05 弹出“正在配置”页面，配置成功后弹出“恭喜您”字样，表明配置成功，如下图所示。



Step 06 单击“完成”按钮，即可完成电子邮件的配置，如下图所示。

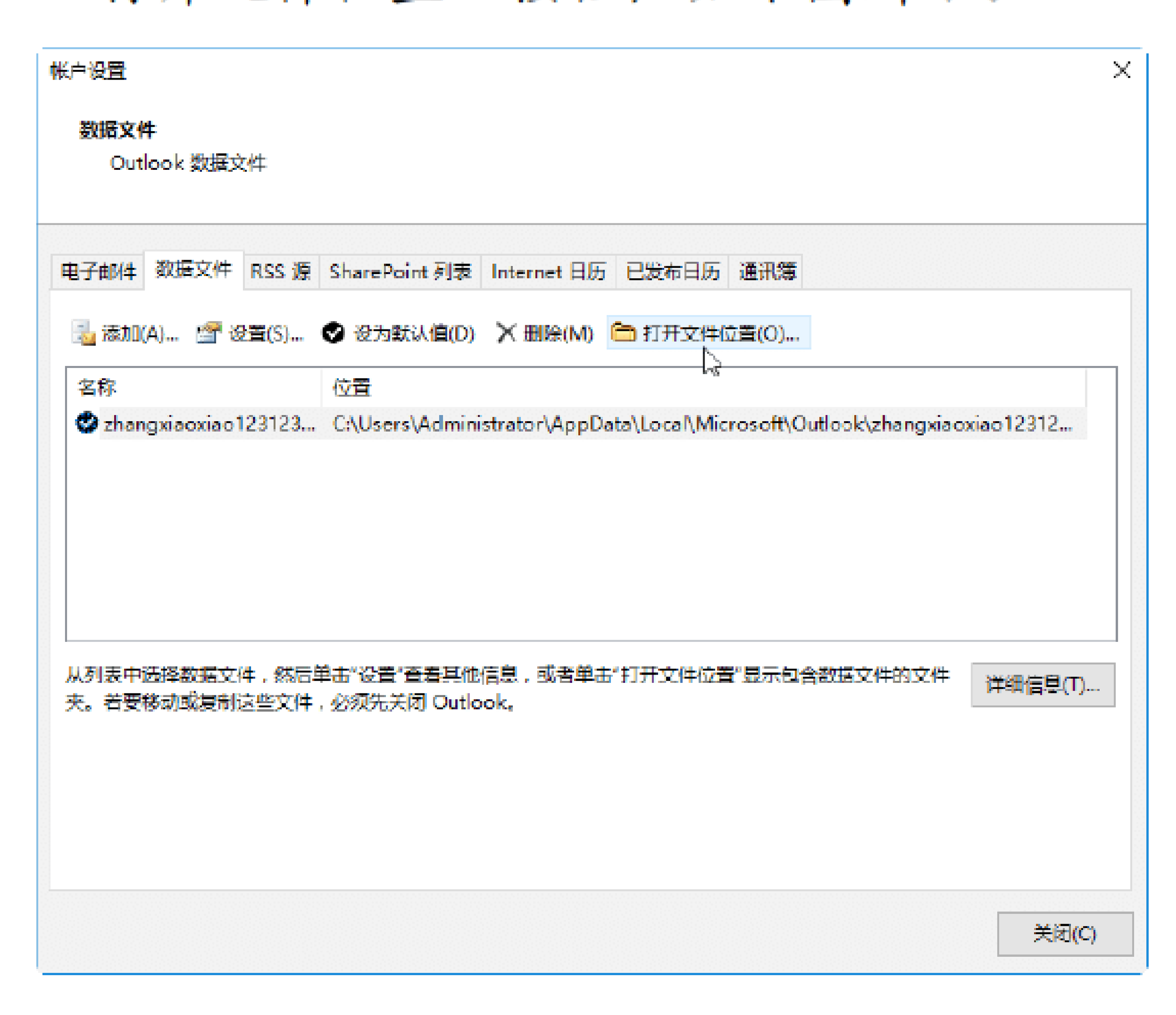


实战演练2——通过账户设置来备份与恢复邮件

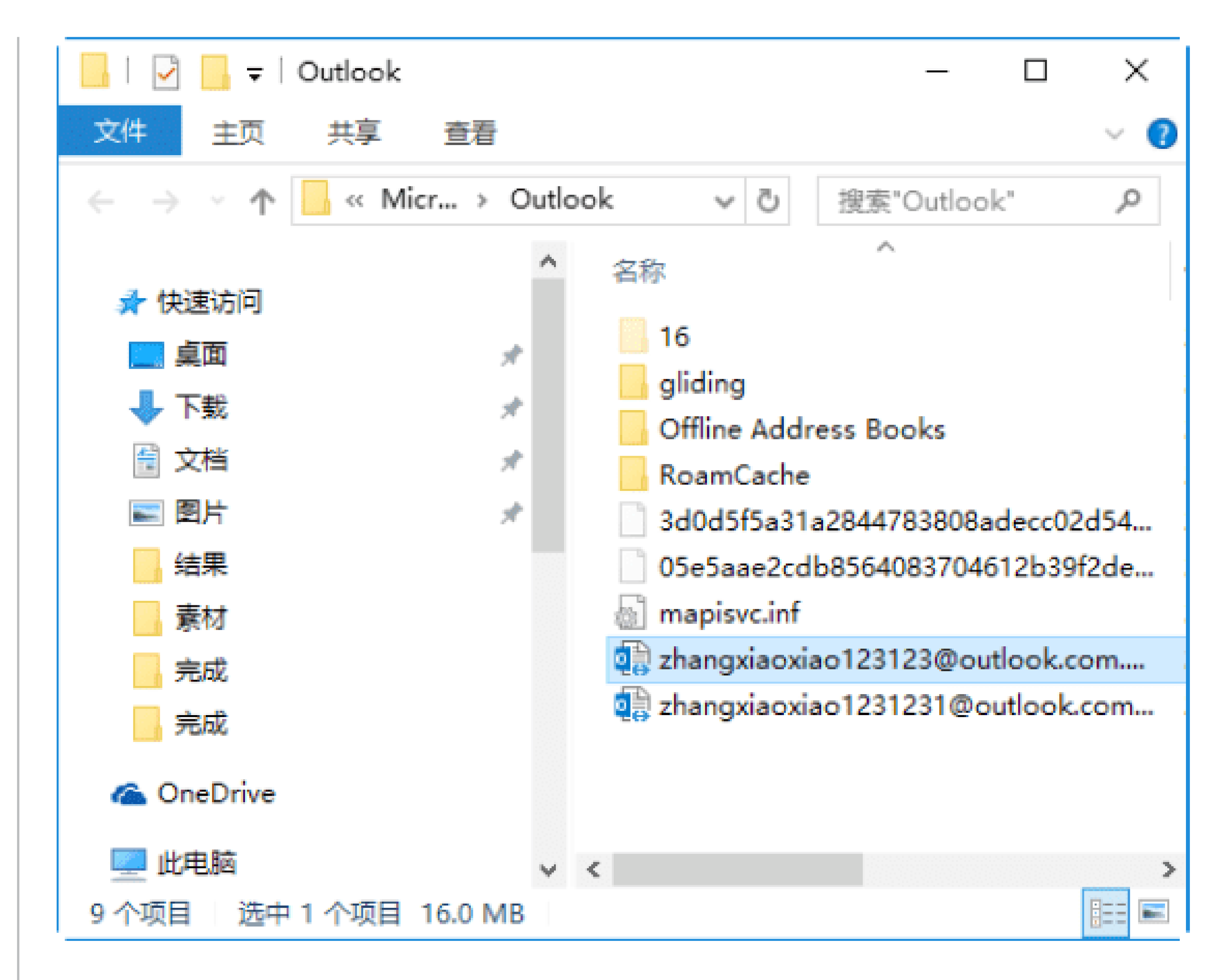
邮件已成为与客户沟通及工作安排等重要传输途径，邮件的重要性已不言而喻，因此定期地备份邮件可以防止邮件的丢失而带来的重大损失。

备份与恢复重要邮件的具体操作步骤如下。

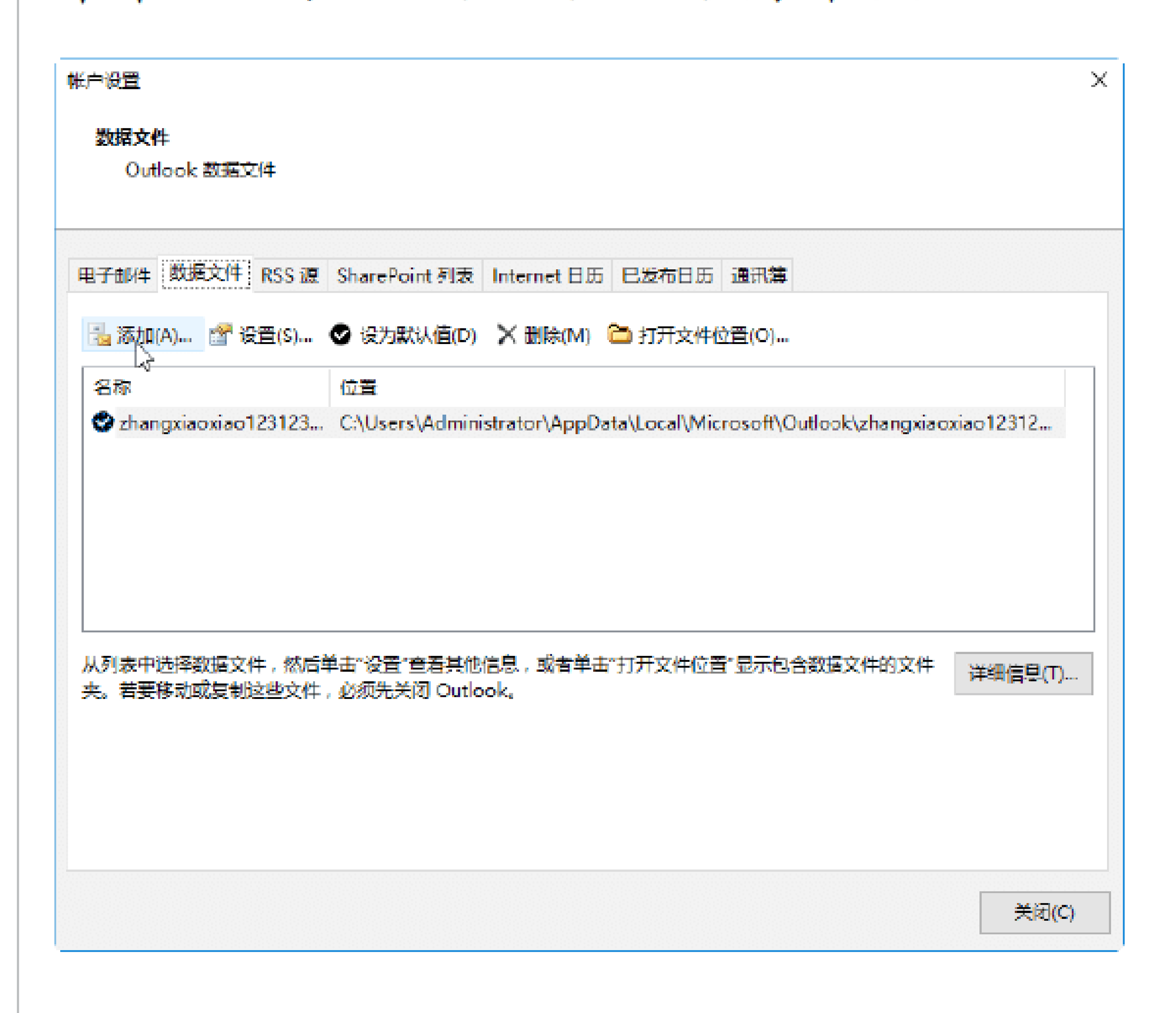
Step 01 选择“文件”选项卡，进入到“文件”界面，然后单击“账户设置”按钮，从弹出的下拉列表中选择“账户设置”选项，打开“账户设置”对话框，在该对话框中选择“数据文件”选项卡，然后单击“打开文件位置”按钮，如下图所示。



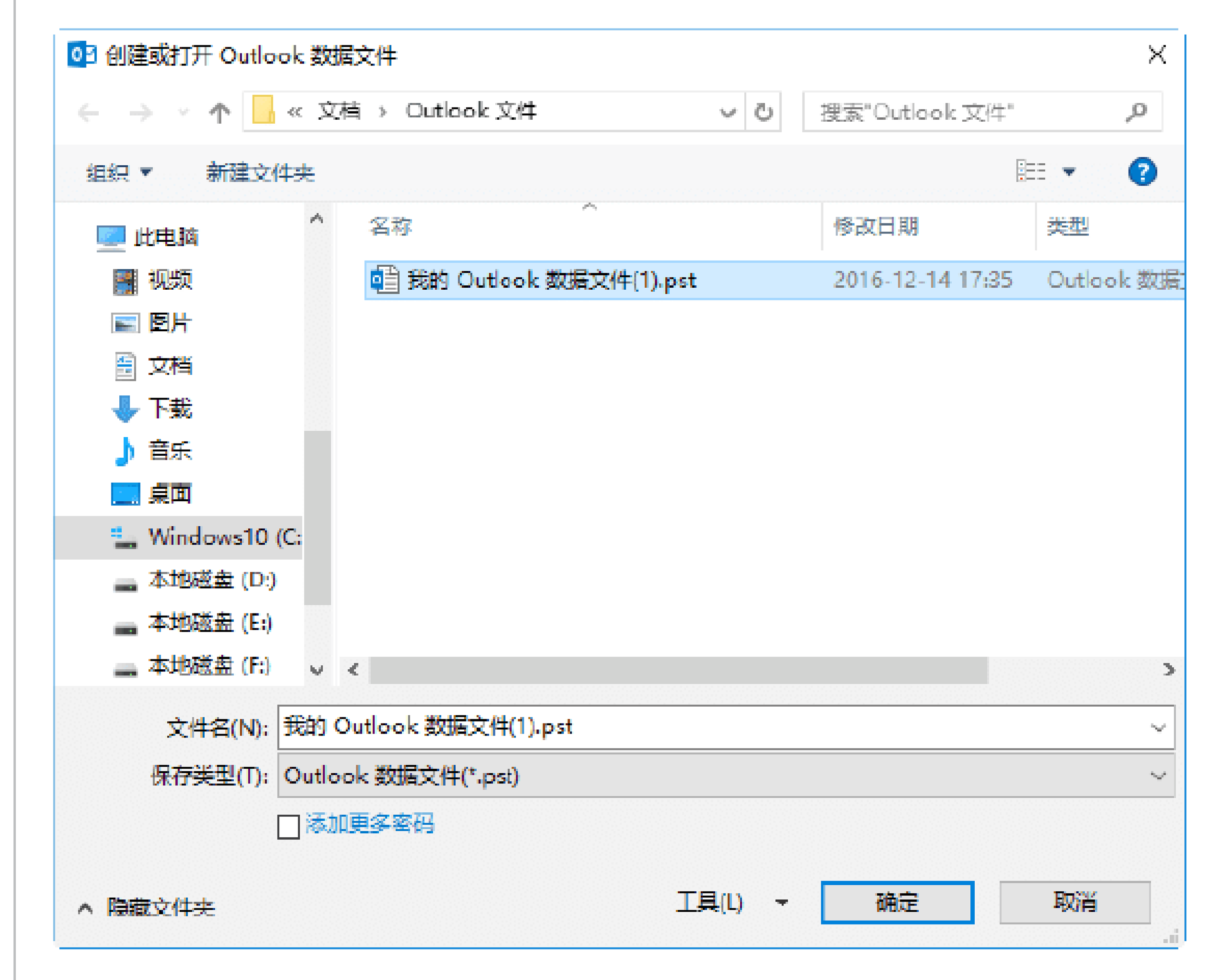
Step 02 根据路径找到Outlook文件夹，将其复制，即可备份邮箱内容，如下图所示。



Step 03 当计算机重装Outlook软件并且需要恢复这些邮件时，在“数据文件”选项卡中单击“添加”按钮，如下图所示。



Step 04 找到文件所在位置进行添加，即可恢复备份的邮件，如下图所示。



12.5　小试身手

练习1：通过向导备份电子邮件

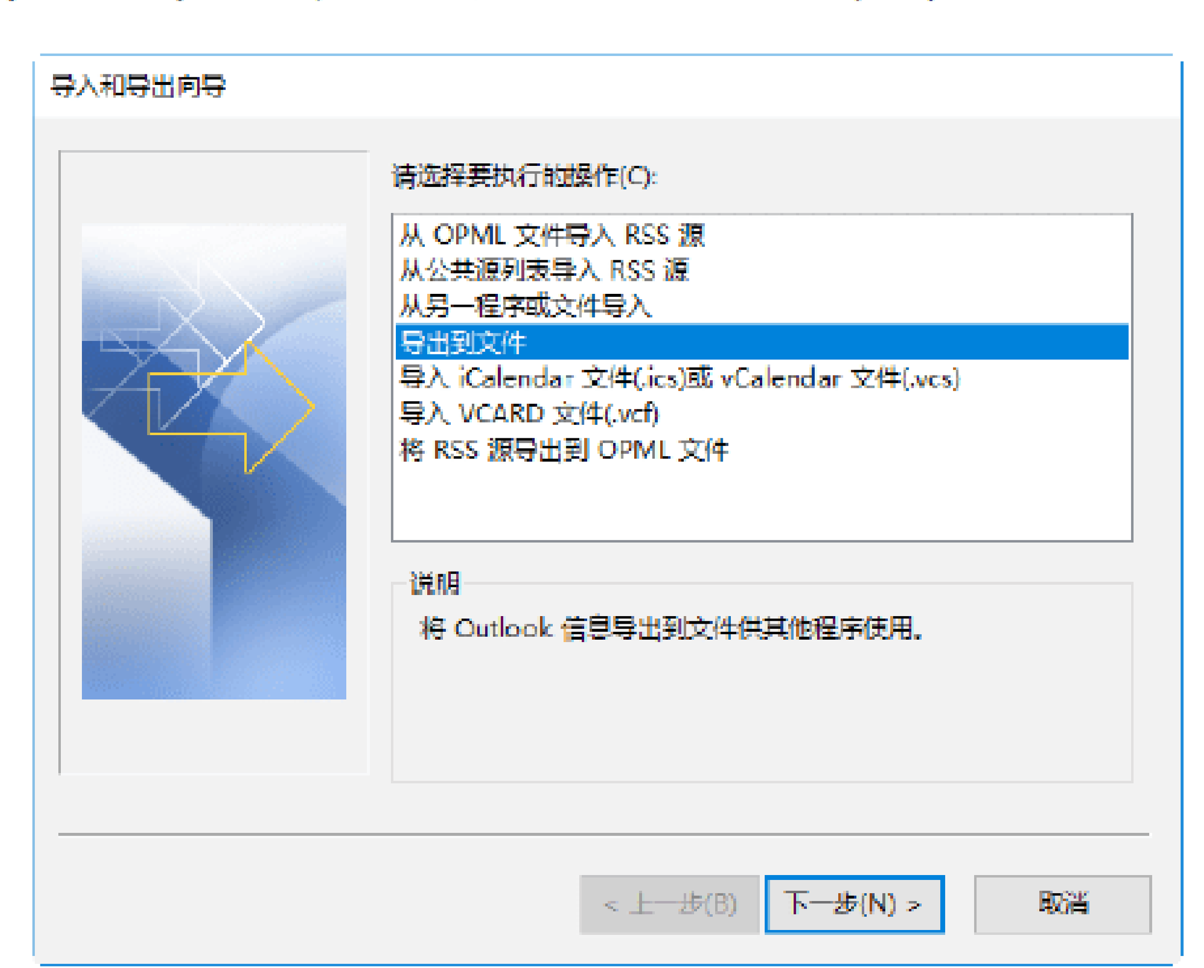
随着网络的日益普及，越来越多的人使用电子邮件进行学习、交流、娱乐以及办公等，显然电子邮件的内容多数是比较重要的信息。因此，为了防止病毒与木马的攻击，导致电子邮件的丢失，对电子邮件进行备份和还原就非常重要了。

使用Outlook中的导入/导出向导功能可以备份电子邮件。具体的操作步骤如下。

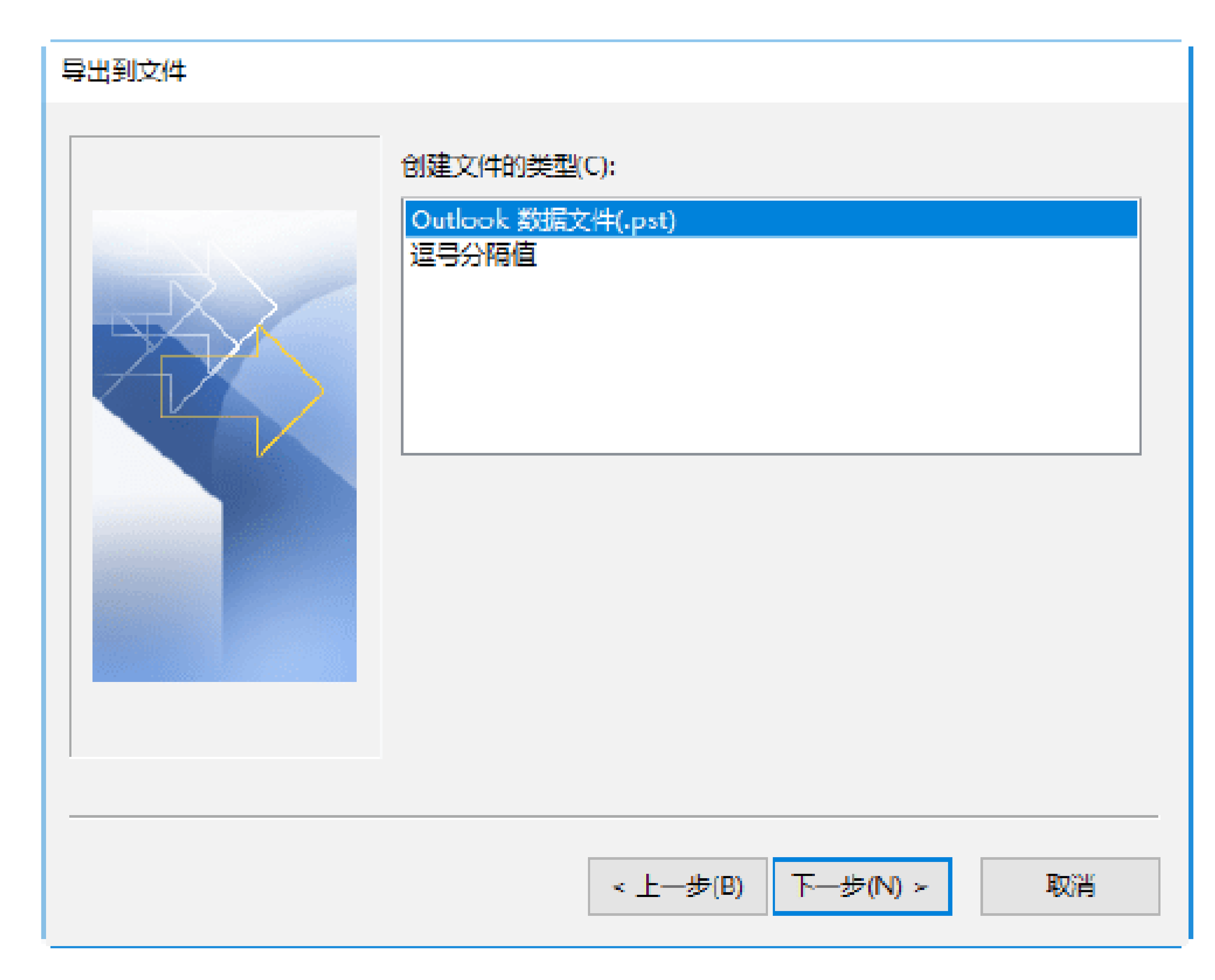
Step 01 启动Outlook 2016主程序，选择“文件”选项卡，进入到“文件”界面，在该界面中选择“打开和导出”选项区域内的“导入/导出”选项，如下图所示。



Step 02 打开“导入和导出向导”对话框，在“请选择要执行的操作”列表框中选择“导出到文件”选项，如下图所示。

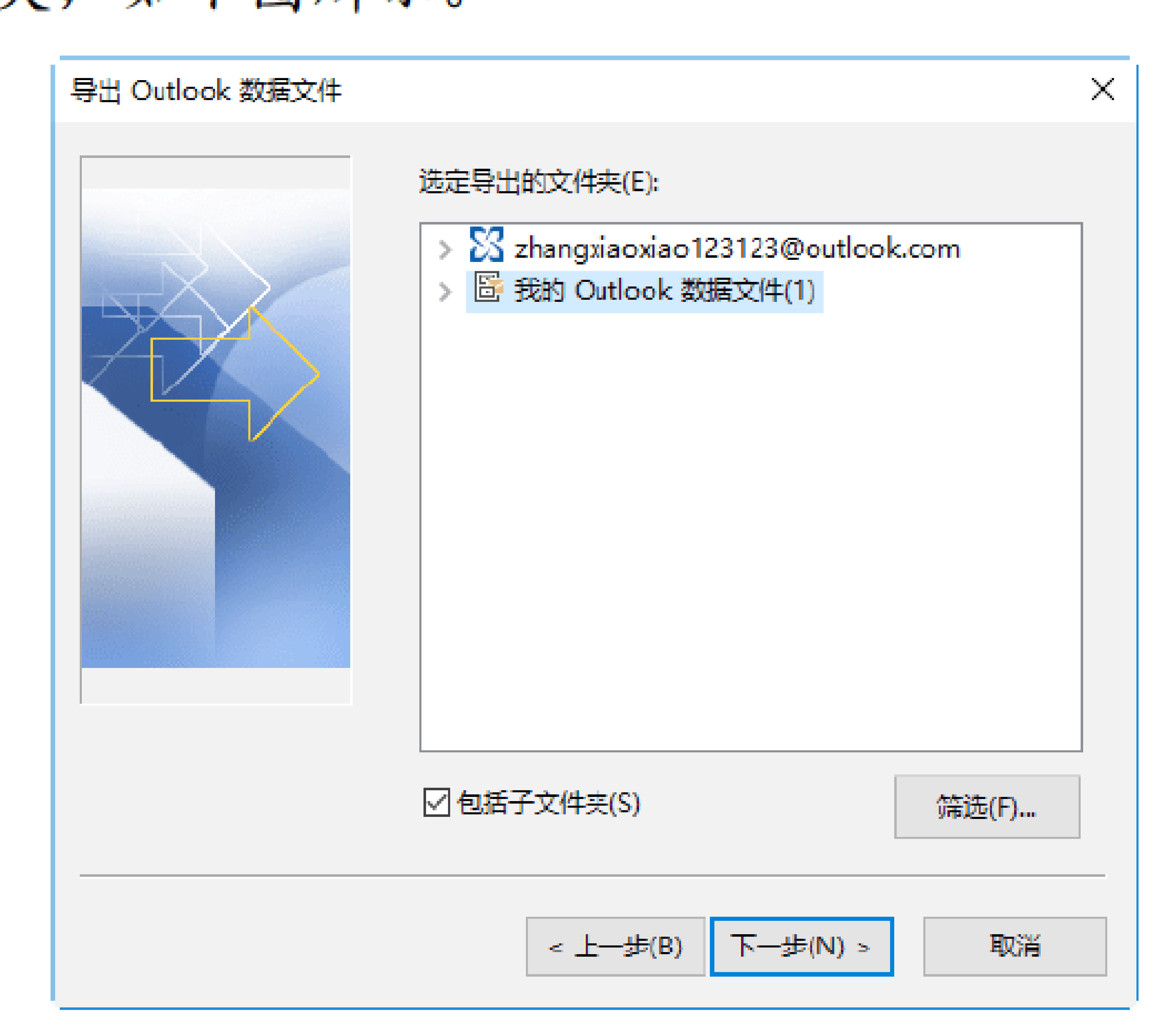


Step 03 单击“下一步”按钮，打开“导出到文件”对话框，在“创建文件的类型”列表框中选择“Outlook 数据文件（pst）”选项，如下图所示。

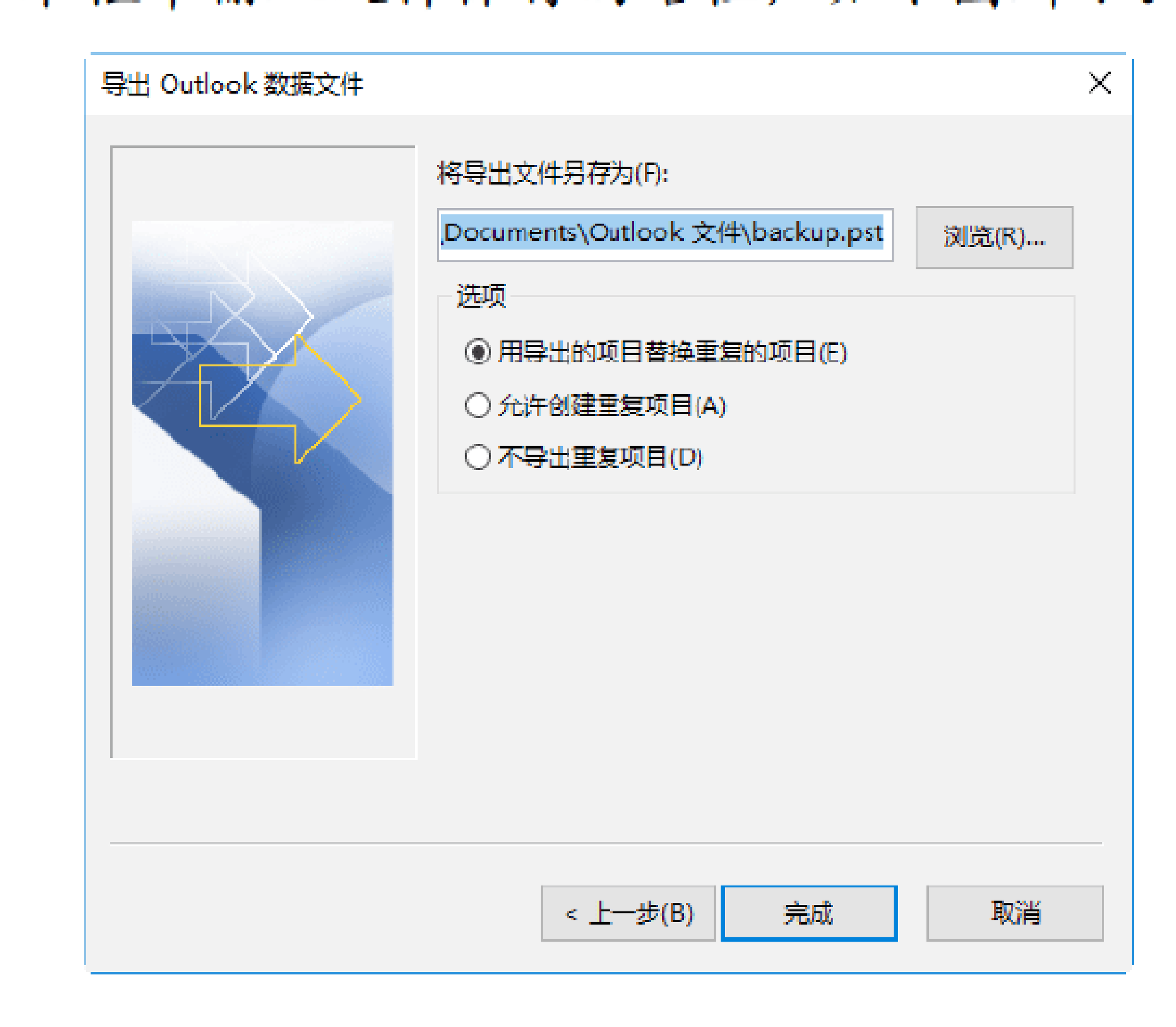




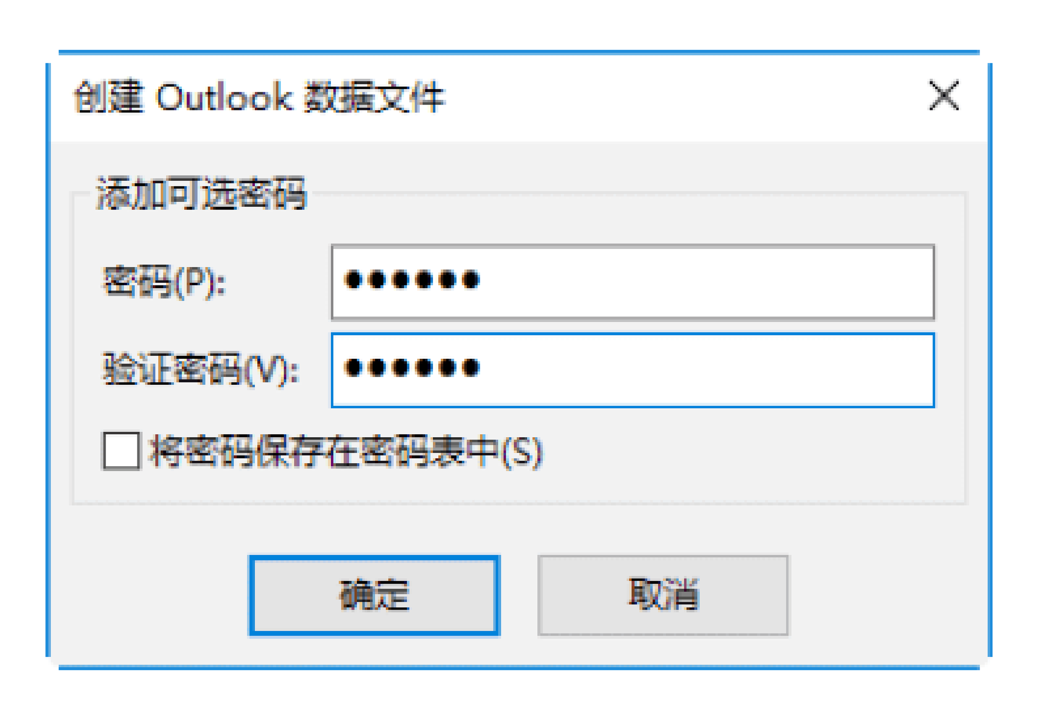
Step 04 单击“下一步”按钮，打开“导出Outlook数据文件”对话框，在“选定导出的文件夹”列表框中选择要导出的文件夹，如下图所示。



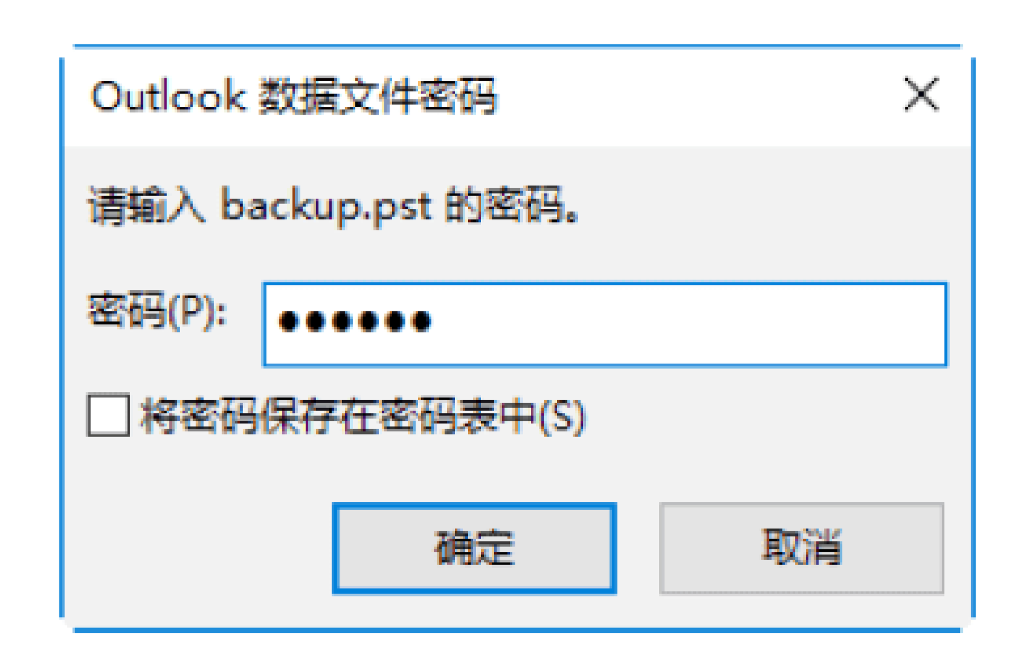
Step 05 单击“下一步”按钮，打开“导出Outlook数据文件”对话框，在“选项”列表中选中“用导出的项目替换重复的项目”单选按钮，在“将导出文件另存为”下的文本框中输入文件保存的路径，如下图所示。



Step 06 单击“完成”按钮，打开“创建Outlook数据文件”对话框，在“密码”和“验证密码”文本框中输入相同的文件密码，如下图所示。



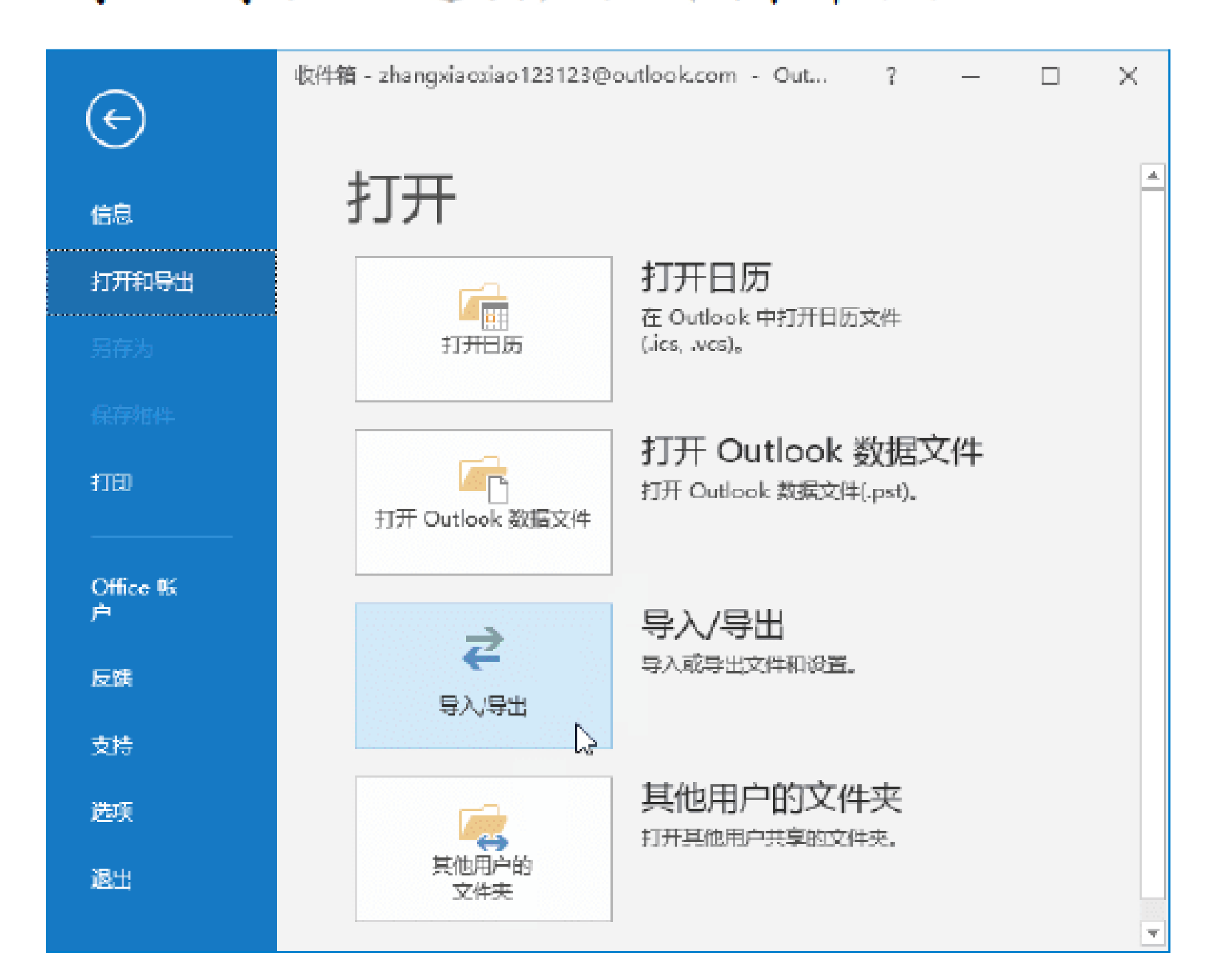
Step 07 单击“确定”按钮，打开“Outlook数据文件密码”对话框，在“密码”中输入文件的密码，如下图所示。单击“确定”按钮，即可完成备份电子邮件的操作。



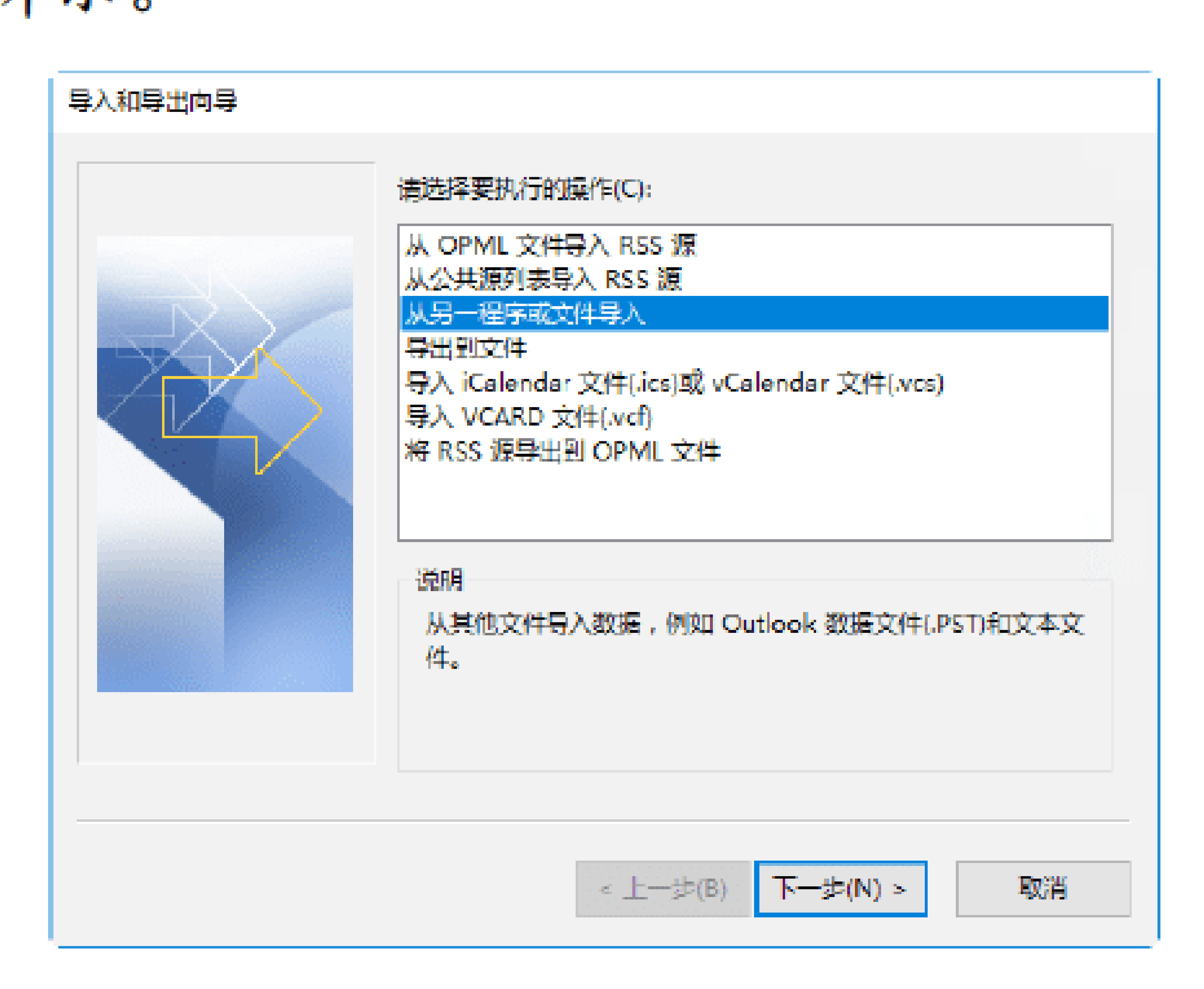
练习2：使用向导还原电子邮件

当电子邮件丢失或受到木马病毒入侵后，可以使用备份的电子邮件来还原。使用向导还原电子邮件的操作步骤如下。

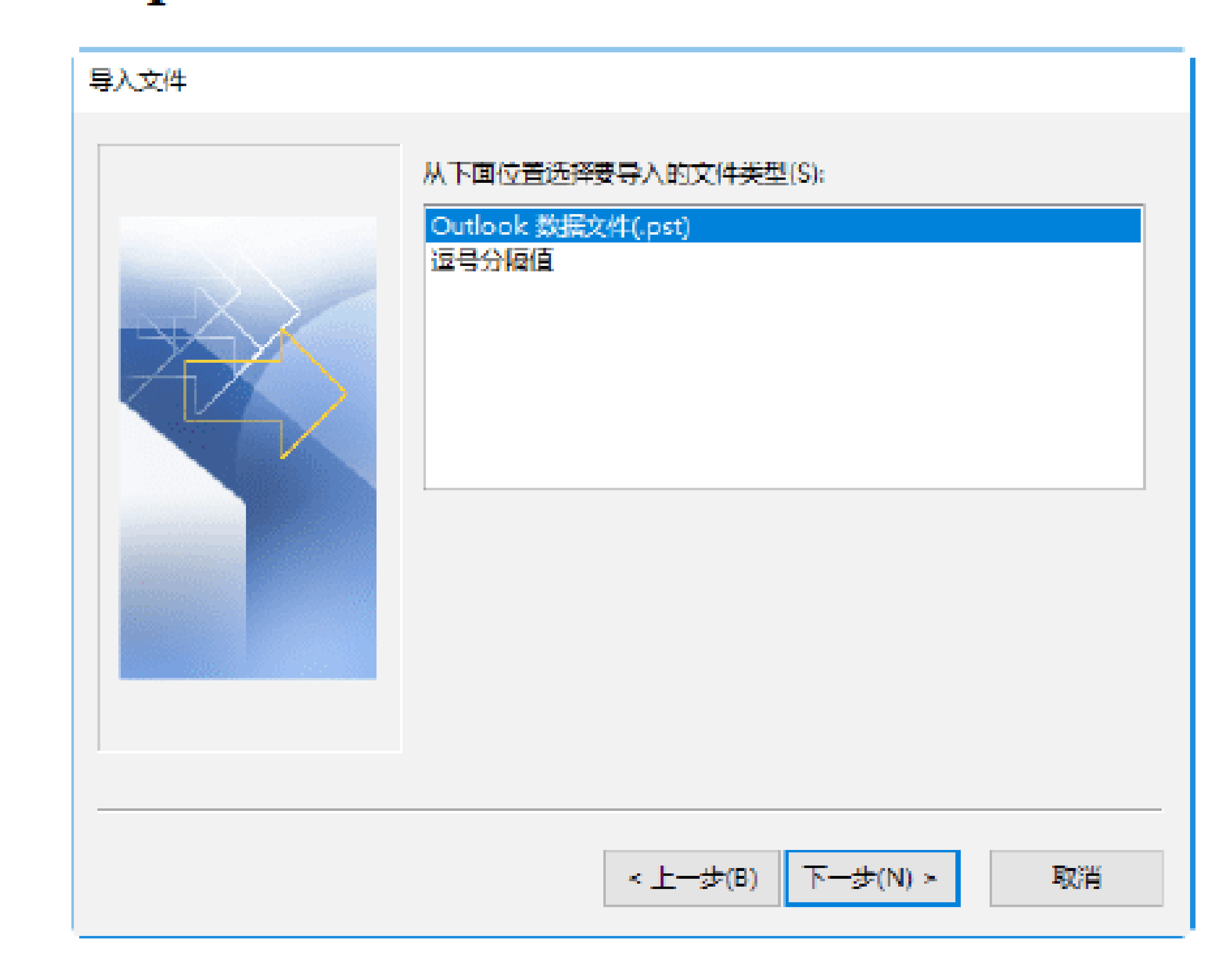
Step 01 启动Outlook 2016主程序，选择“文件”选项卡，进入到“文件”界面，在该界面中选择“打开和导出”选项区域内的“导入/导出”选项，如下图所示。



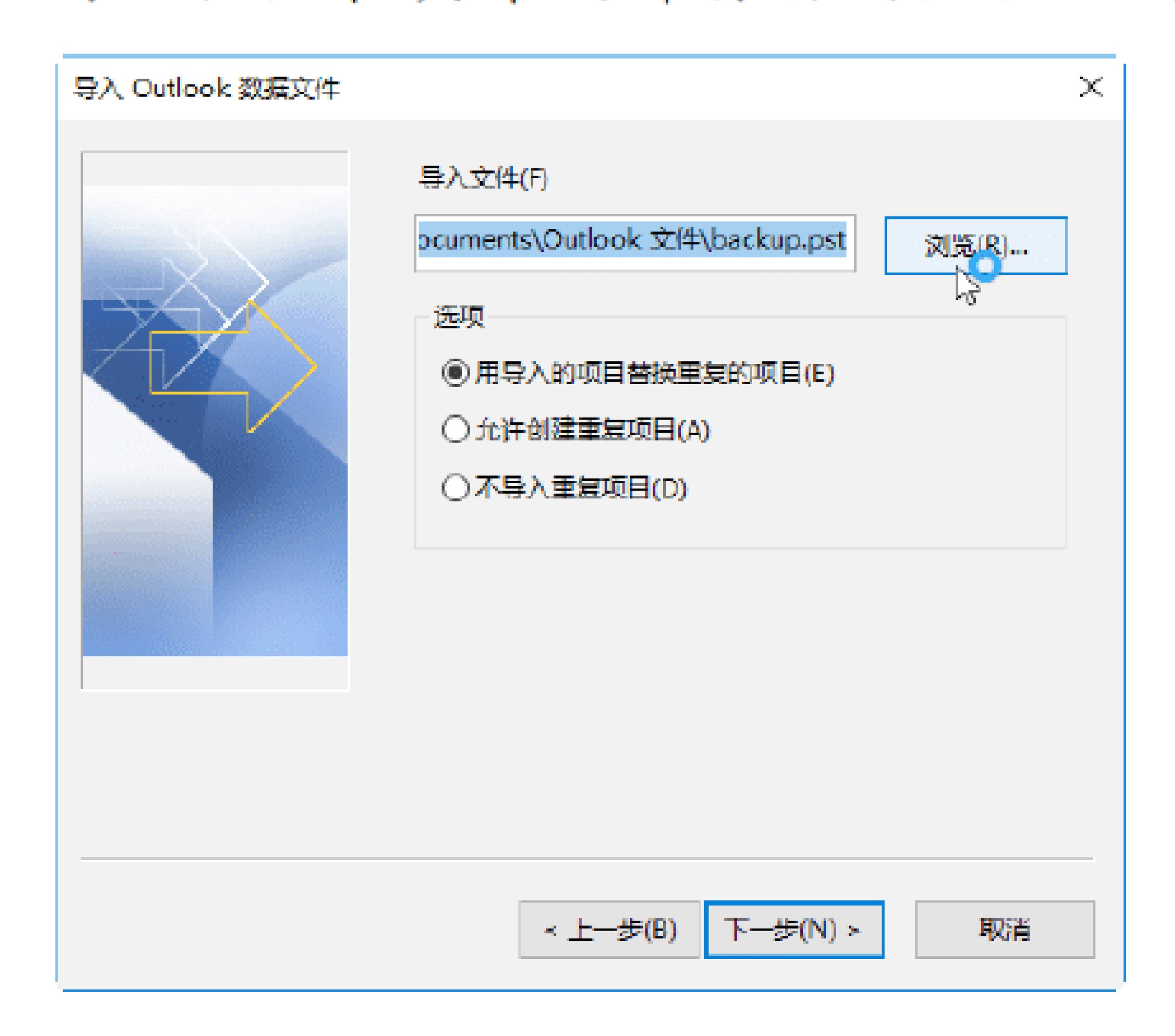
Step 02 打开“导入和导出向导”对话框，在“请选择要执行的操作”列表框中选择“从另一个程序或文件导入”选项，如下图所示。



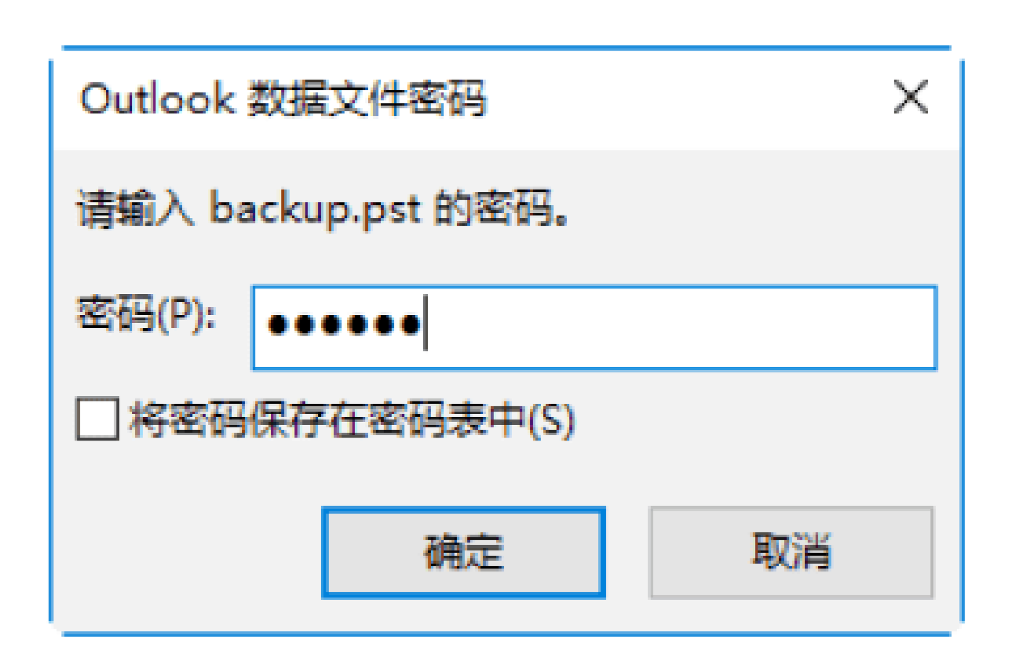
Step 03 单击“下一步”按钮，打开“导入文件”对话框，在“从下面位置选择要导入的文件类型”对话框中选择“Outlook 数据文件（pst）”选项，如下图所示。



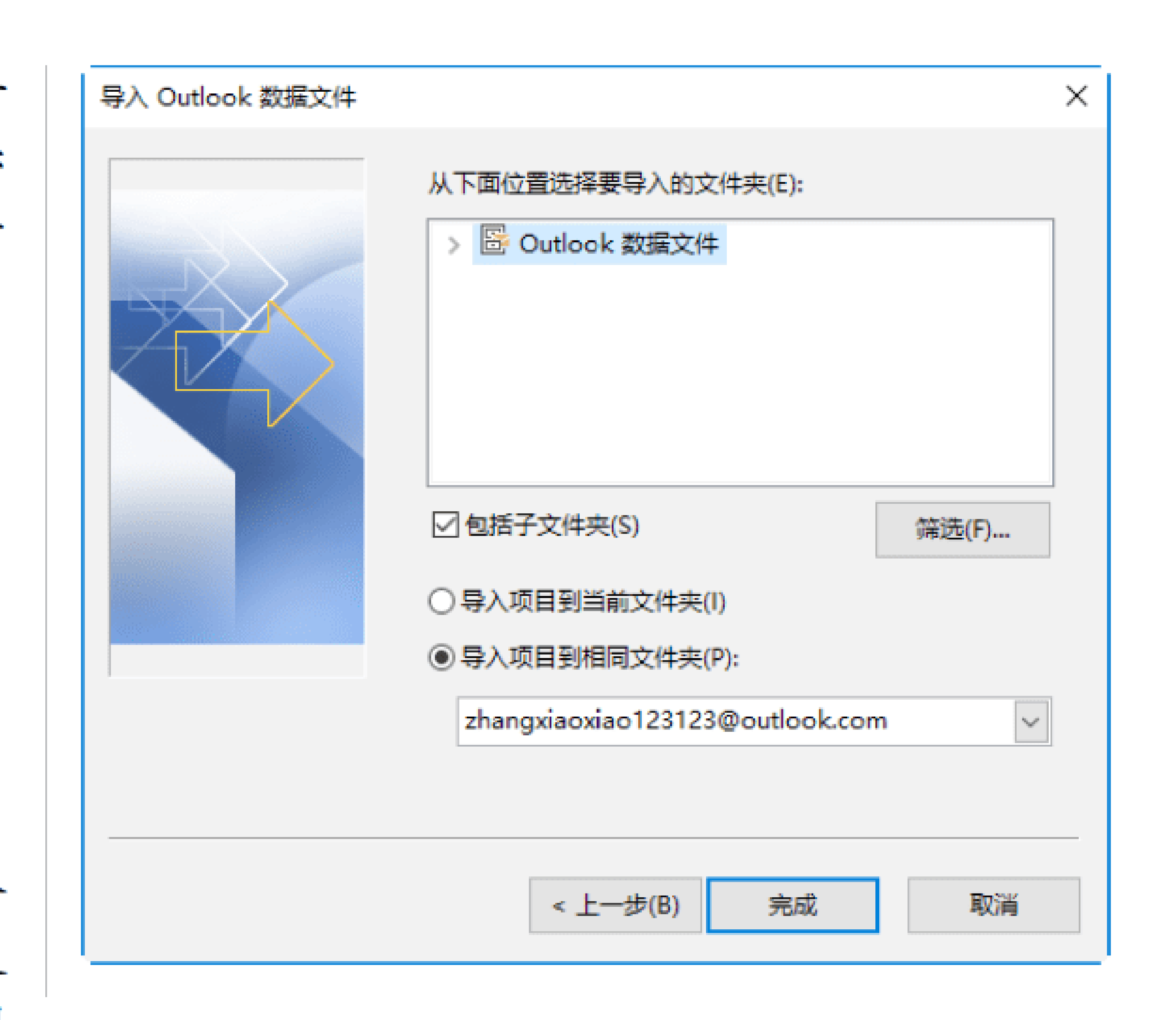
Step 04 单击“下一步”按钮，打开“导入Outlook数据文件”对话框，在“选项”列表中选中“用导入的项目替换重复的项目”单选按钮，在“导入文件”下的文本框中输入导入文件的路径，如下图所示，或单击“浏览”按钮，打开“打开Outlook数据文件”对话框，在其中选择备份的数据文件。



Step 05 单击“下一步”按钮，打开“Outlook数据文件密码”对话框，在“密码”文本框中输入数据文件的密码，如下图所示。



Step 06 单击“确定”按钮，打开“导入Outlook数据文件”对话框，选择需要恢复的邮件，单击“完成”按钮即可，如下图所示。



第13章　操作系统的安全防护

其实很多时候系统不安全不是操作系统或安全软件存在问题，而是用户对系统安全设置不了解，没有设置正确的系统安全策略，从而给了黑客可乘之机。本章将通过设置本地安全策略、设置组策略、设置计算机管理策略和注册表编辑器安全防范等方面，详细介绍系统安全策略设置知识。

13.1　通过清理间谍软件保护系统安全

间谍软件是一种能够在用户不知情的情况下，在其计算机上安装后门、收集用户信息的软件。间谍软件以恶意后门程序的形式存在，该程序可以打开端口、启动FTP服务器，或者搜集击键信息并将信息反馈给攻击者。



实战1：使用“反间谍专家”清理

使用“反间谍专家”可以扫描系统薄弱环节以及全面扫描硬盘，智能检测和查杀超过上万种木马、蠕虫、间谍软件等，终止它们的恶意行为。当检测到可疑文件时，该工具还可以将其隔离，从而保护系统的安全。

下面介绍使用“反间谍专家”工具的基本步骤。

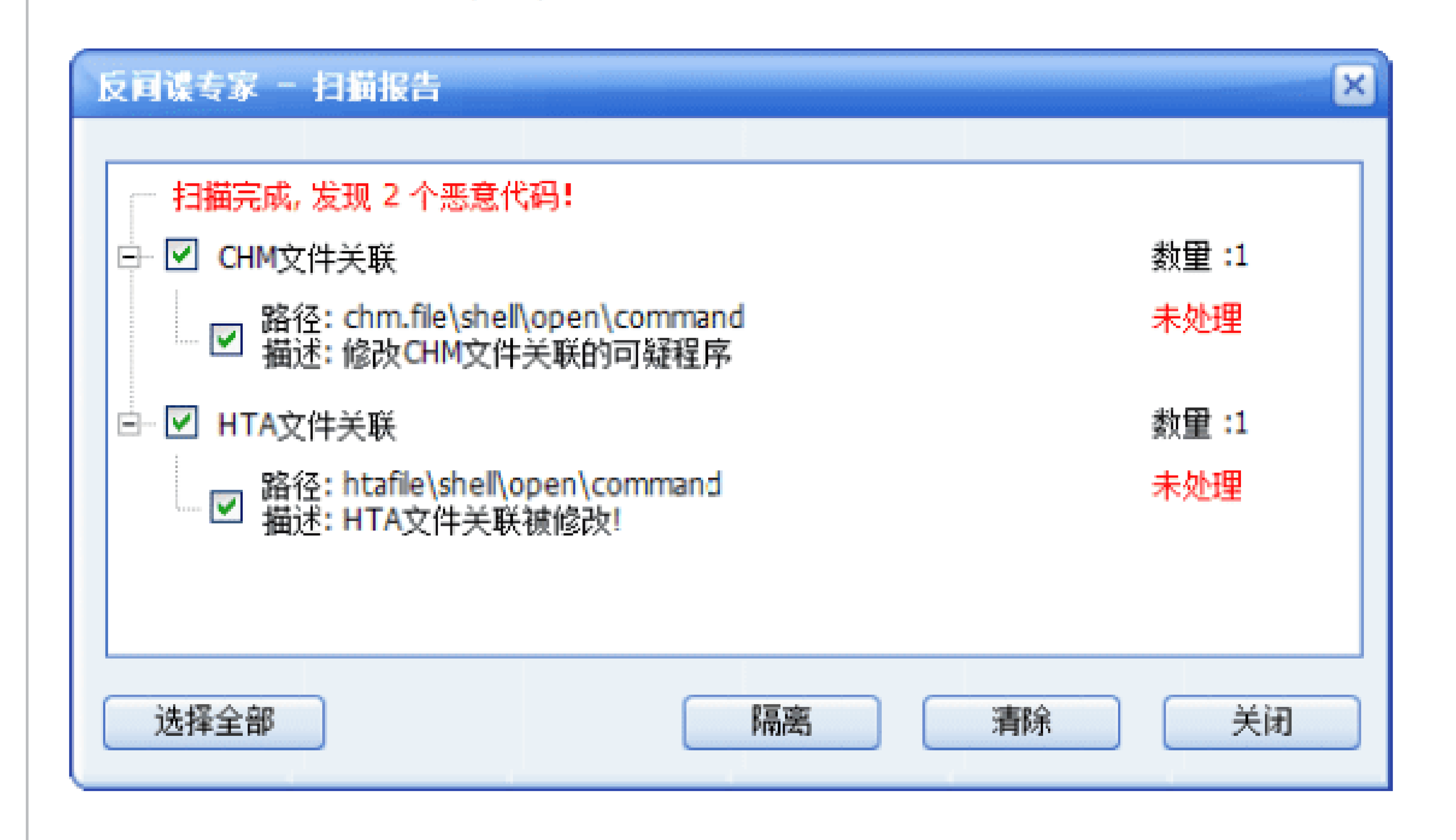
Step 01 运行“反间谍专家”程序，即可打开“反间谍专家”主界面，从中可以看出“反间谍专家”有“快速查杀”和“完全查杀”两种方式，如下图所示。



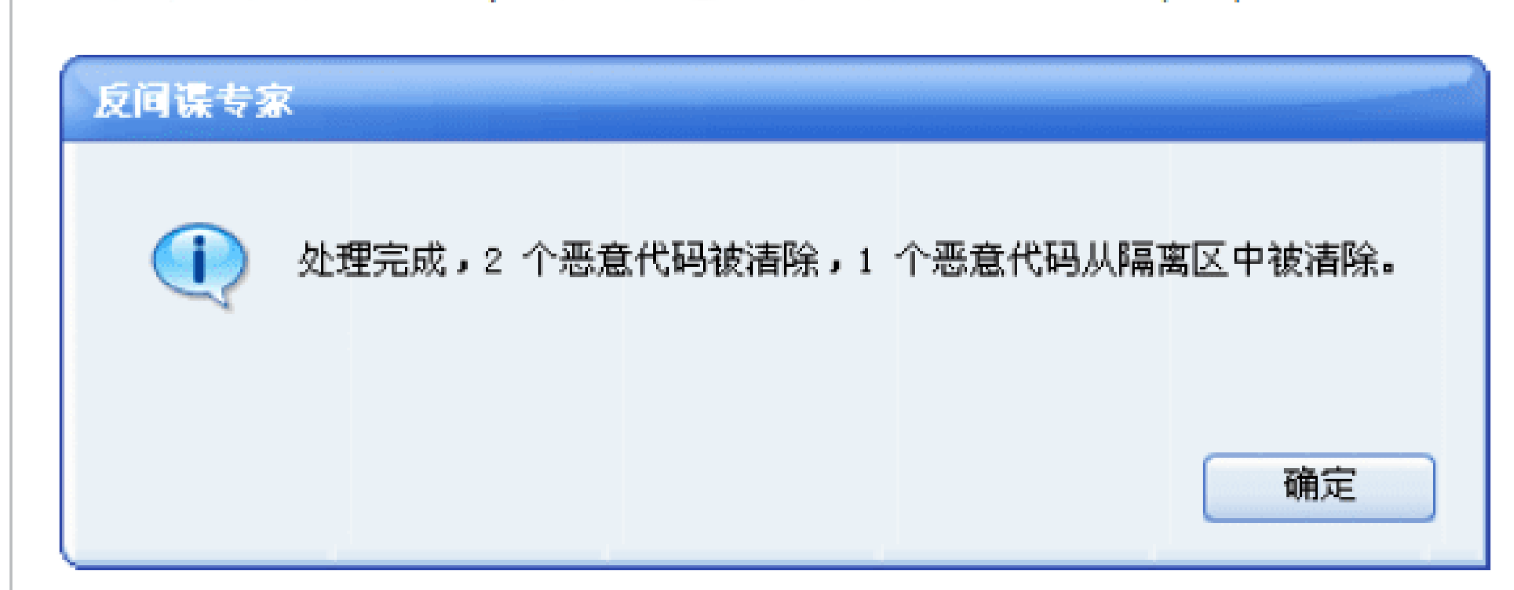
Step 02 在“查杀”栏目中单击“快速查杀”按钮，然后在右边的窗口中单击“开始查杀”按钮，即可打开“扫描状态”对话框，如下图所示。



Step 03 在扫描结束之后，即可打开“扫描报告”对话框，在其中列出了扫描到的恶意代码，如下图所示。



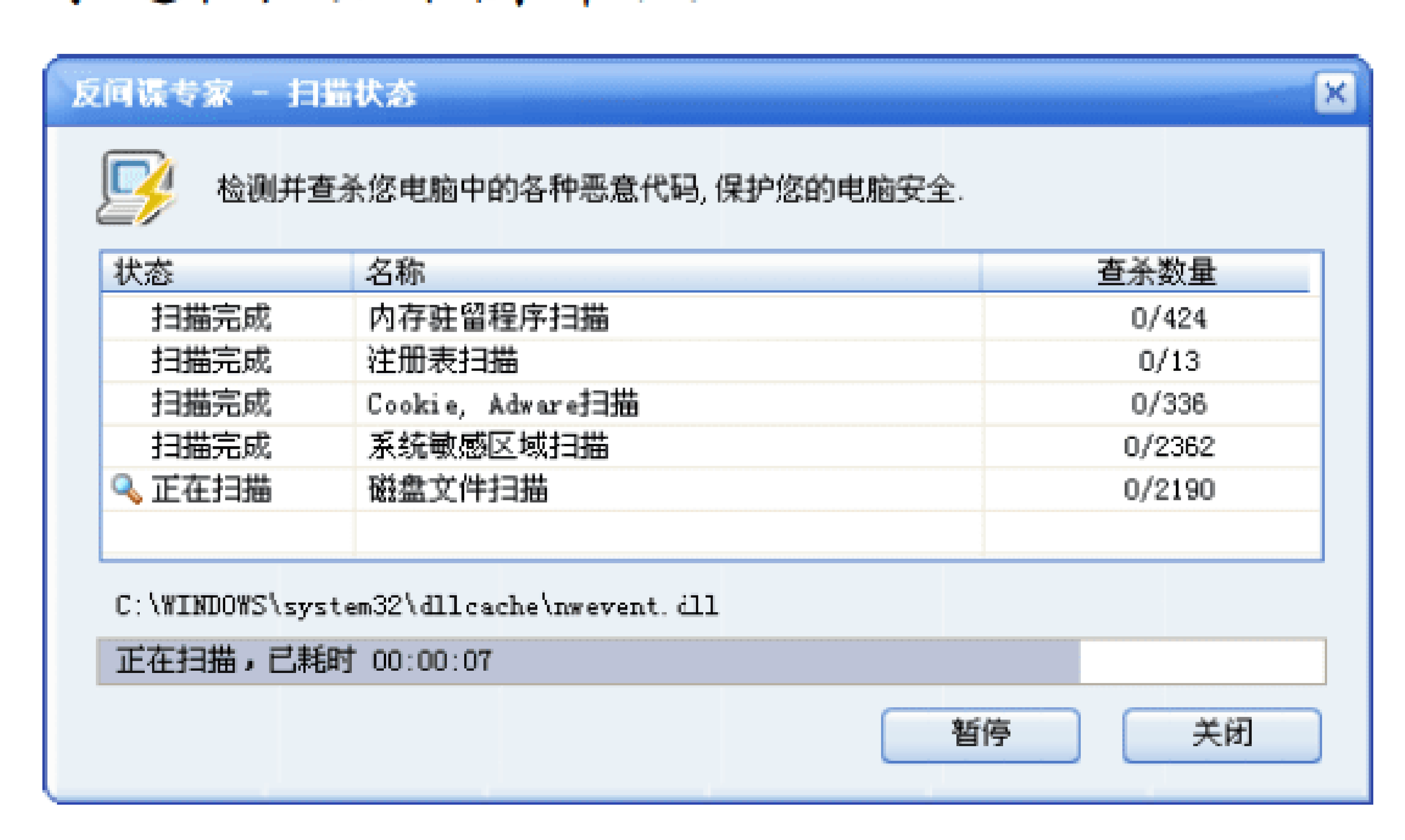
Step 04 单击“选择全部”按钮，即可选中全部的恶意代码，单击“清除”按钮，即可快速杀除扫描到的恶意代码，如下图所示。



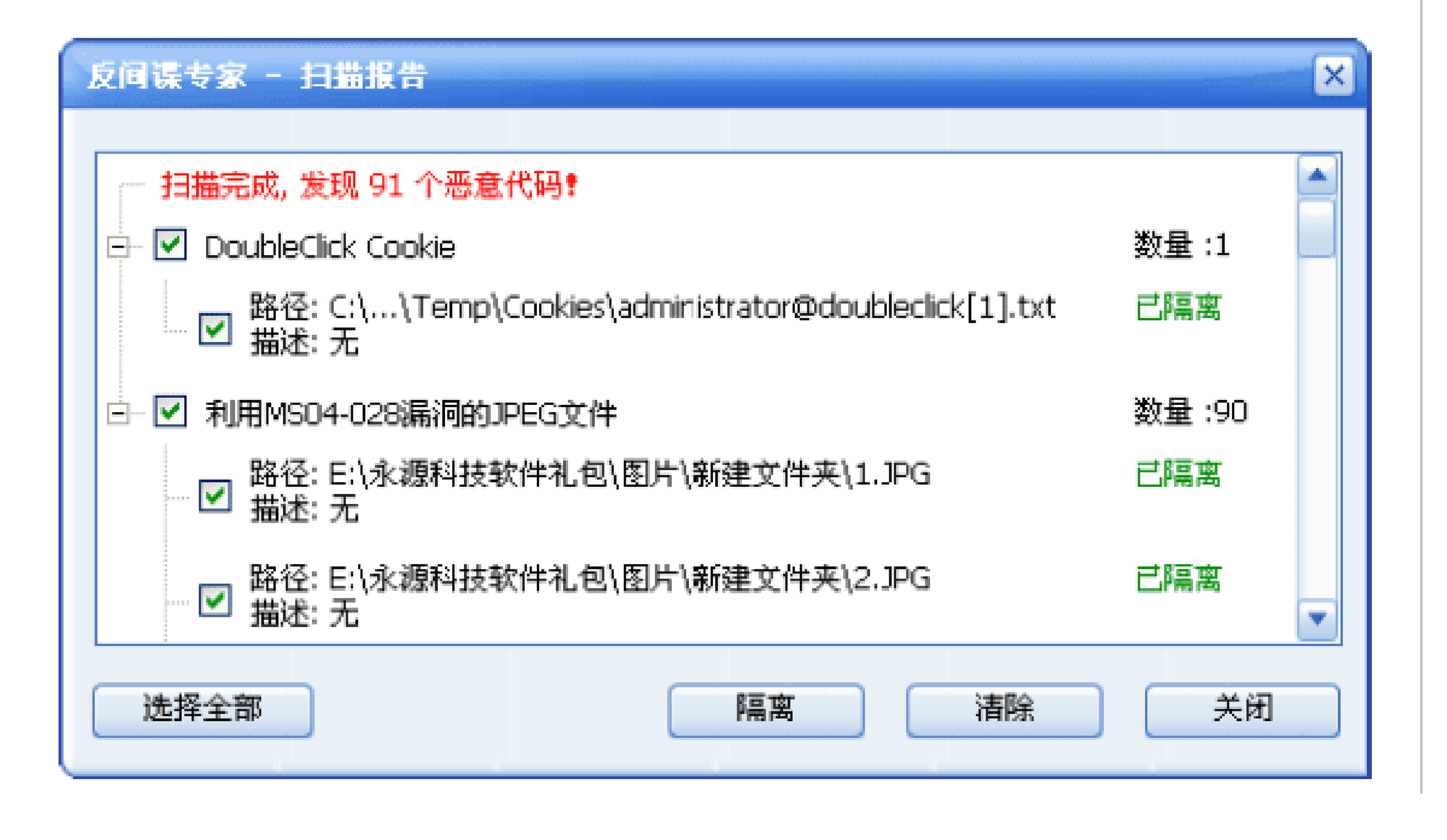
Step 05 如果要彻底扫描并查杀恶意代码，则需采用“完全查杀”方式。在“反间谍专家”主窗口中，单击“完全查杀”按钮，即可打开“完全查杀”对话框。从中可以看出完全查杀有3种快捷方式供选择，这里选中“扫描本地硬盘中的所有文件”单选按钮，如下图所示。



Step 06 单击“开始查杀”按钮，即可打开“扫描状态”对话框，在其中可以查看查杀进程，如下图所示。



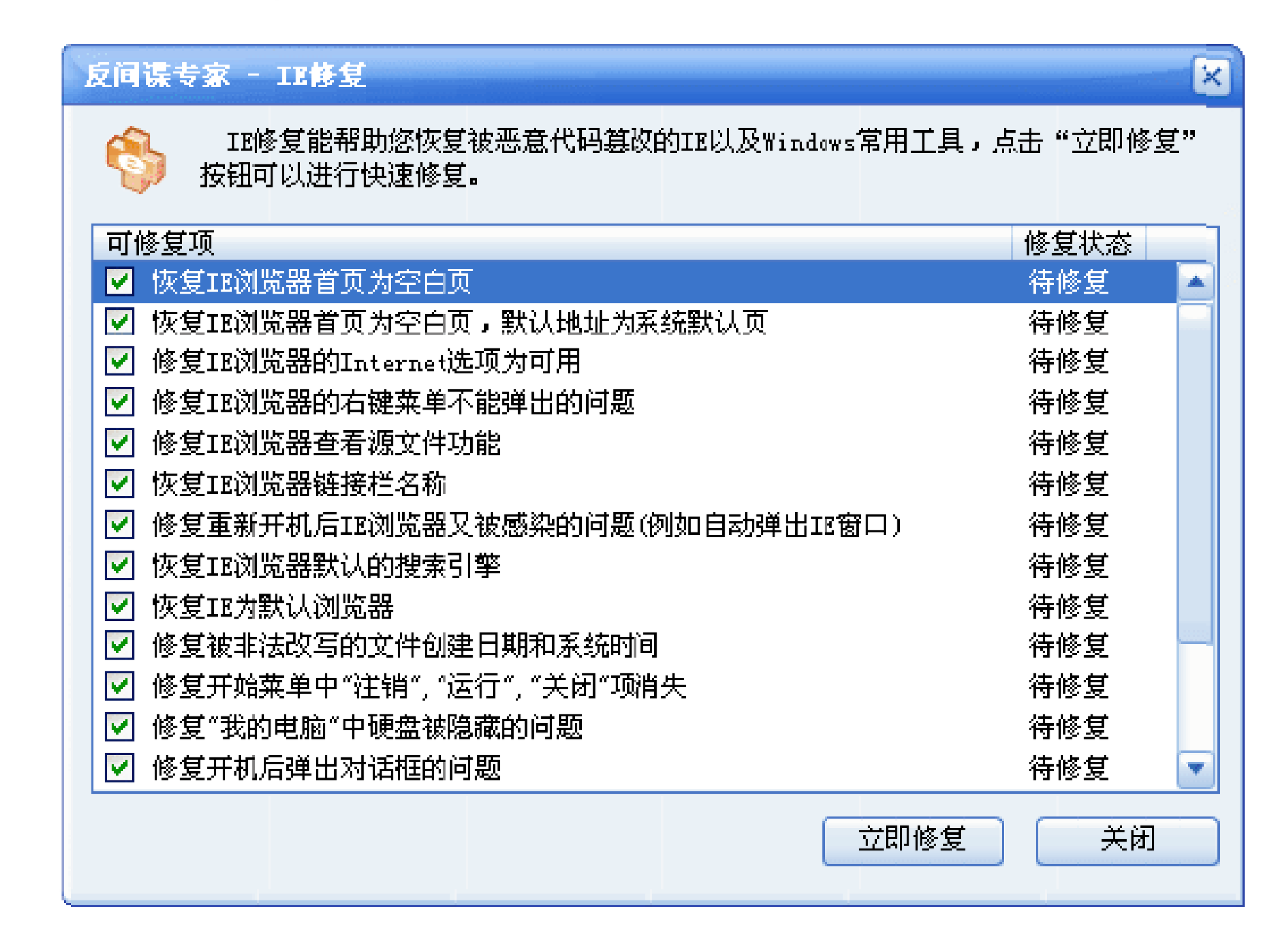
Step 07 待扫描结束之后，即可打开“扫描报告”对话框，在其中列出所扫描到的恶意代码，如下图所示。勾选要清除的恶意代码前面的复选框后，单击“清除”按钮，即可删除这些恶意代码。



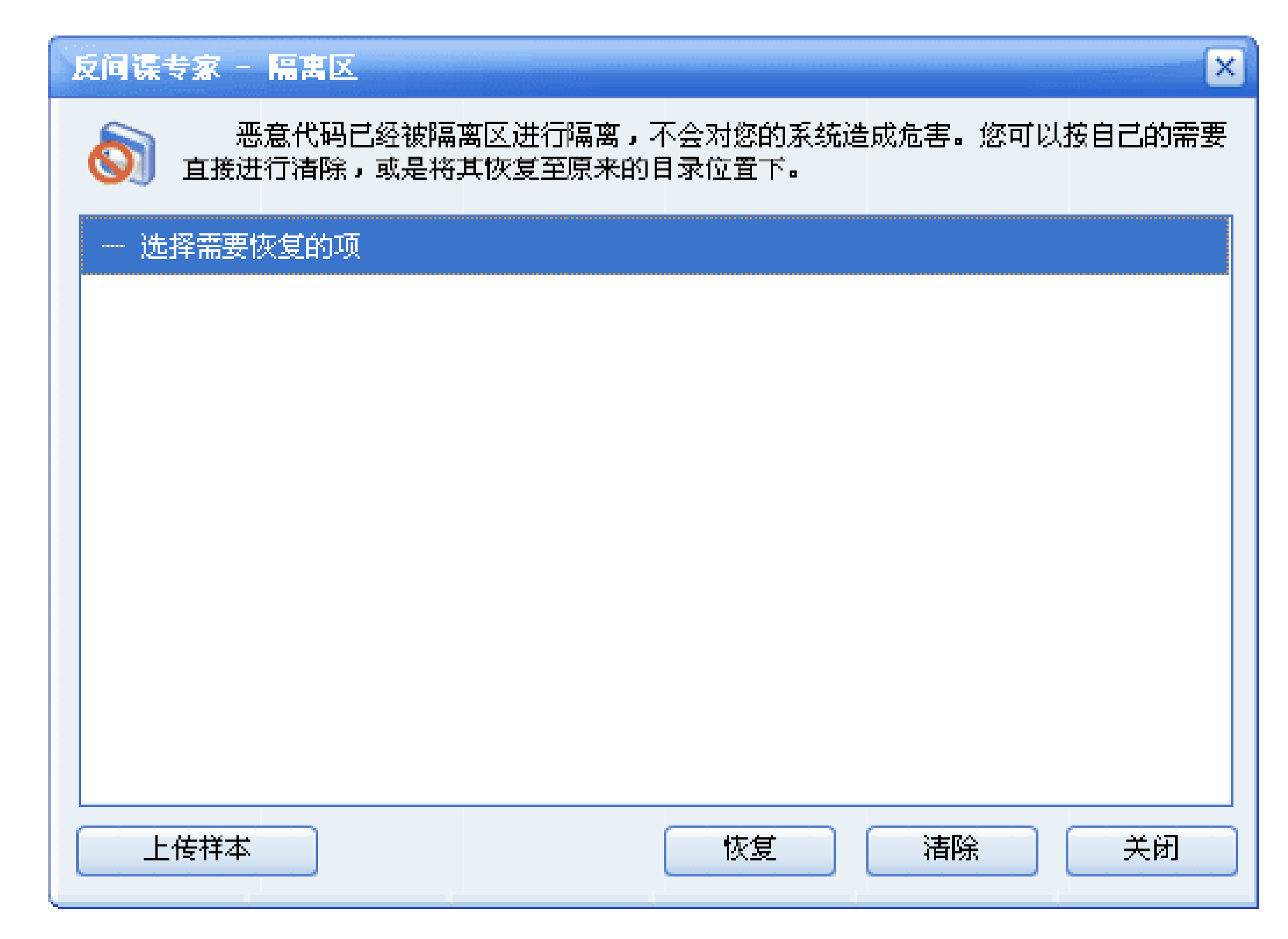
Step 08 在“反间谍专家”主界面中切换到“常用工具”栏目中，单击“系统免疫”按钮，打开“系统免疫”对话框，单击“启用”按钮，即可确保系统不受到恶意程序的攻击，如下图所示。



Step 09 单击“IE修复”按钮，即可打开“IE修复”对话框，选择需要修复的项目，如下图所示，单击“立即修复”按钮，即可将IE恢复到其原始状态。



Step 10 单击“隔离区”按钮，则可查看已经隔离的恶意代码，选择隔离的恶意项目，可以对其进行恢复或清除操作，如下图所示。



Step 11 单击“高级工具”功能栏，即可进入“高级工具”设置界面，如下图所示。



Step 12 单击“进程管理”按钮，即可打开“进程管理器”对话框，在其中对进程进行相应的管理，如下图所示。



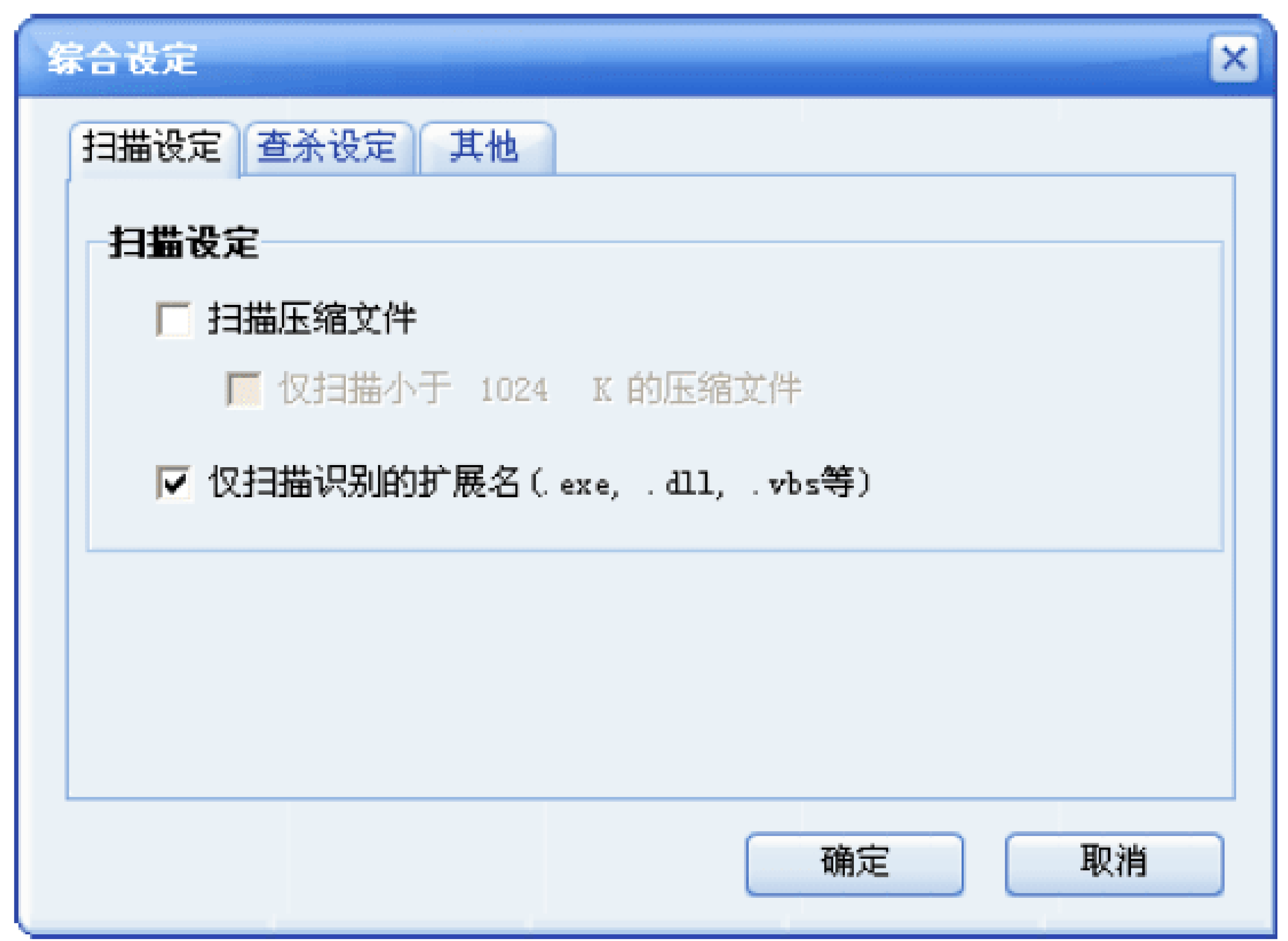
Step 13 单击“服务管理”按钮，即可打开“服务管理器”对话框，在其中对服务进行相应的管理，如下图所示。



Step 14 单击“网络连接管理”按钮，即可打开“网络连接管理器”对话框，在其中对网络连接进行相应的管理，如下图所示。



Step 15 选择“工具”→“综合设定”选项，即可打开“综合设定”对话框，在其中对扫描设定进行相应的设置，如下图所示。

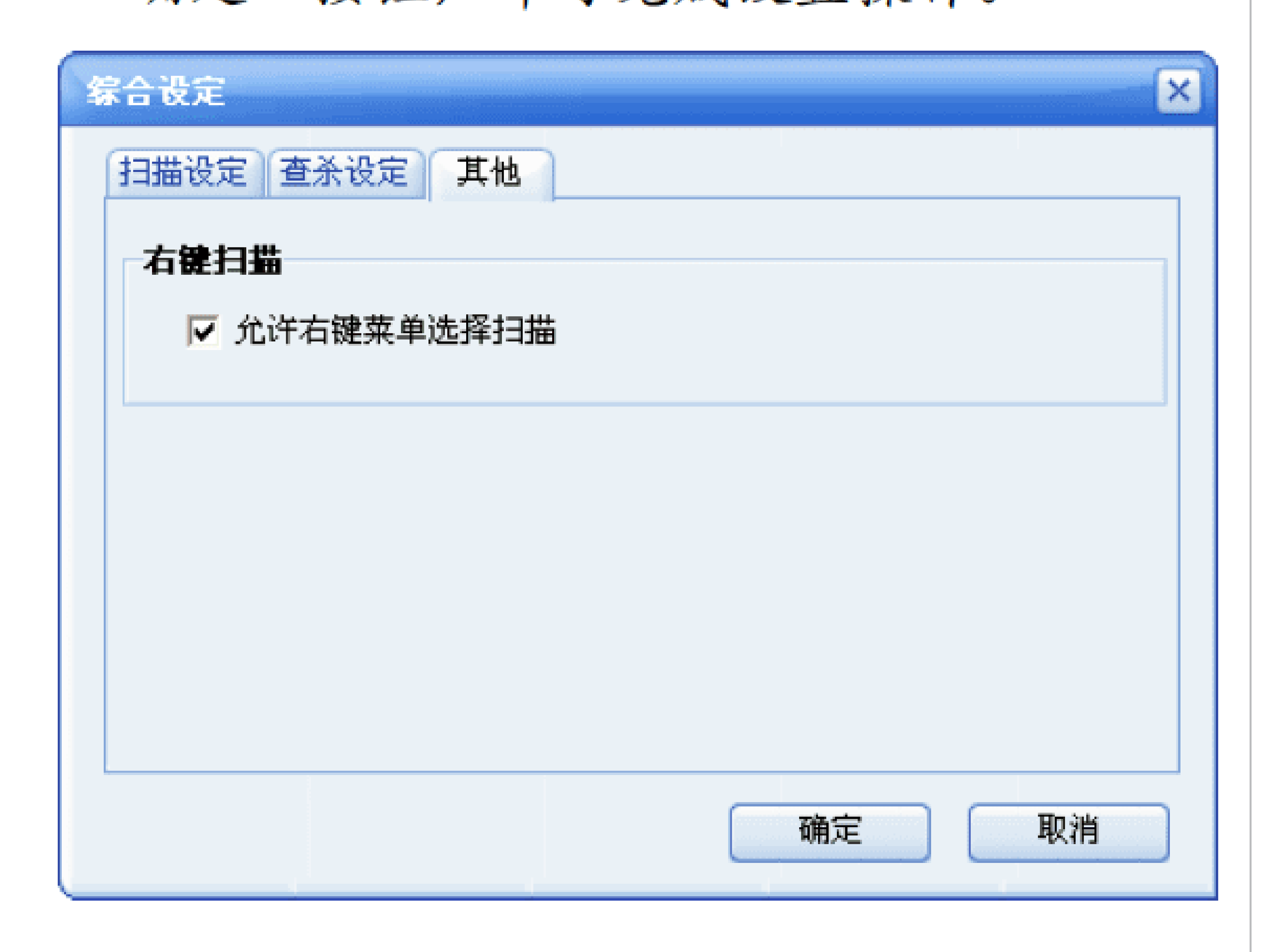


Step 16 选择“查杀设定”选项卡，即可进入“查杀设定”设置界面，在其中设定发现恶意程序时的缺省动作，如下图所示。



Step 17 勾选“其他”选项卡，即可进入“其

他”设置界面，在其中勾选“允许右键菜单选择扫描”复选框，如下图所示，单击“确定”按钮，即可完成设置操作。



实战2：使用“Windows清理助手”清理

“Windows清理助手”是一款可以自定义规则的查杀程序，使用它可以清理网上大部分间谍软件，而且还可以根据用户的需求建立白名单与黑名单，做到完全可自定义是否清理。

使用“Windows清理助手”清理间谍软件的操作步骤如下。

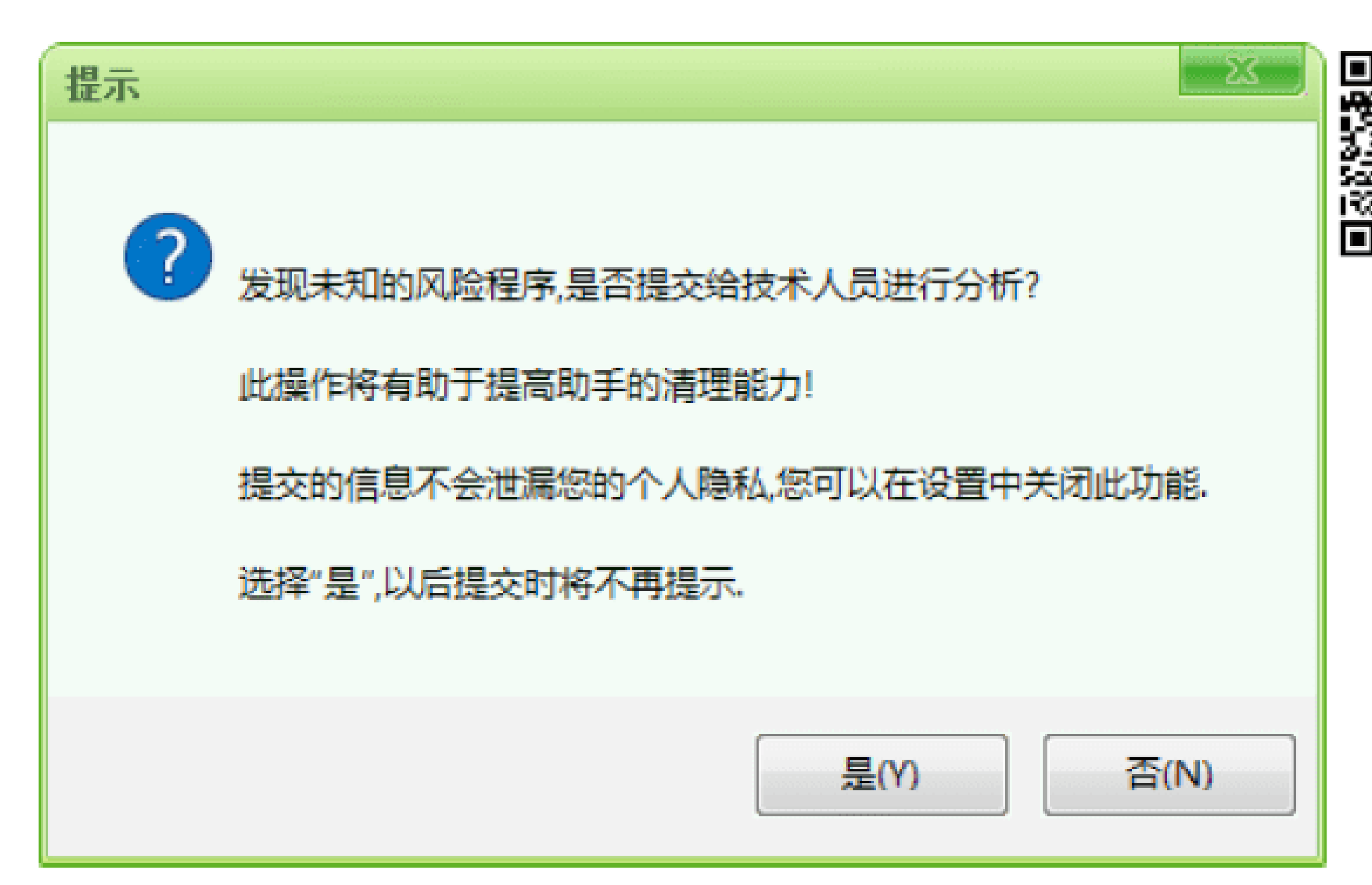
Step 01 双击下载的“Windows清理助手”可执行文件，即可打开“Windows清理助手3.0”工作界面，如下图所示。



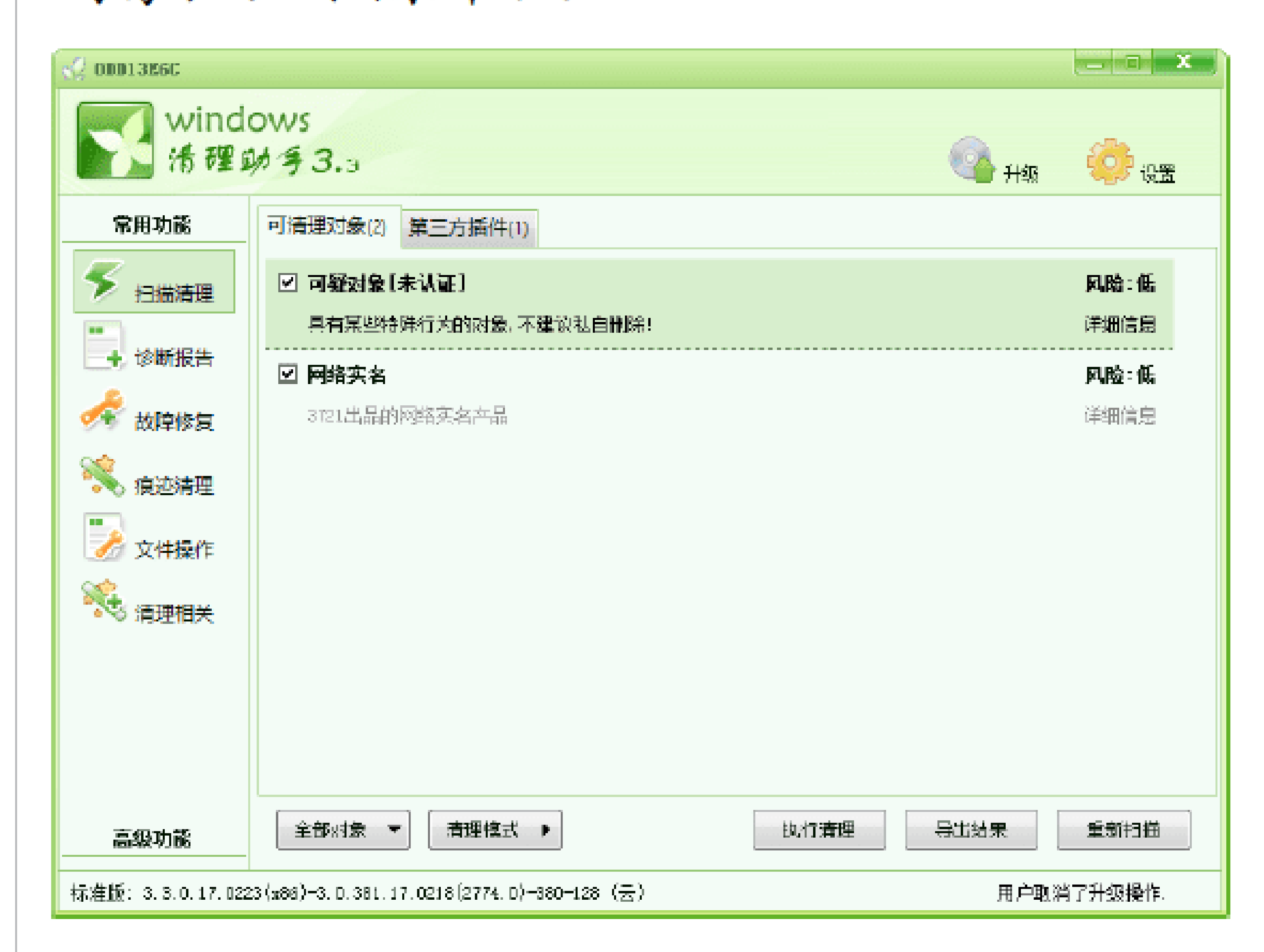
Step 02 单击“立即扫描”按钮，即可开始扫描计算机中的间谍软件，并在下方显示扫描进度条，如下图所示。



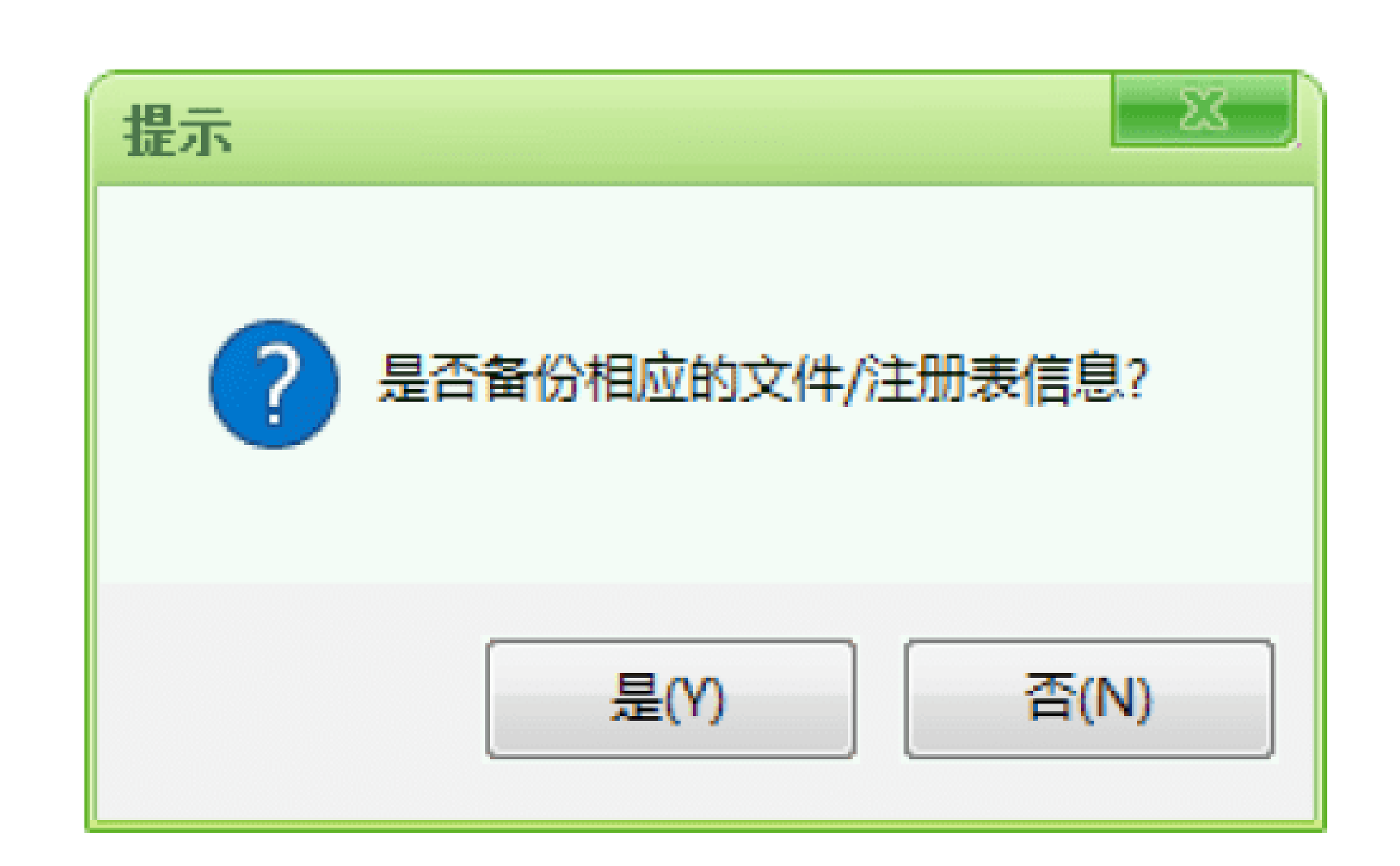
Step 03 扫描完成后，给出相应的提示信息，提示用户发现未知的风险程序，是否提交给技术人员进行分析，这里单击“是”按钮，如下图所示。



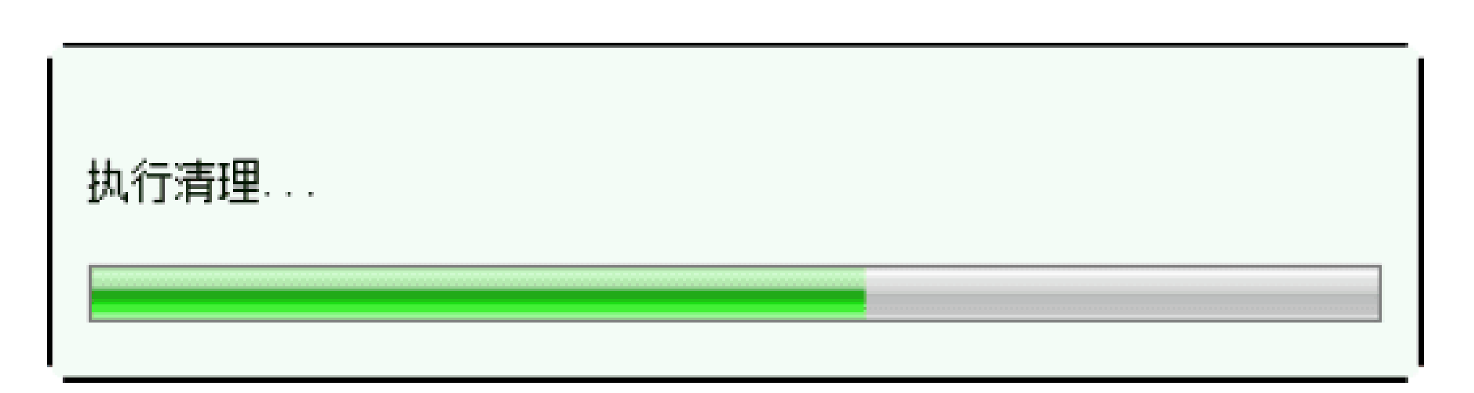
Step 04 分析完成后，返回到“Windows清理助手”工作界面，在其中选择需要清理的对象，如下图所示。



Step 05 单击“执行清理”按钮，弹出一个信息提示框，提示用户“是否备份相应的文件/注册表信息”，这里单击“是”按钮，如下图所示。



Step 06 备份完成后，即可开始清理扫描出来的间谍软件，并显示扫描的进度，如下图所示。



Step 07 在“常用功能”选项列表中选择“诊断报告”选项，进入“诊断报告”工作界面，如下图所示。



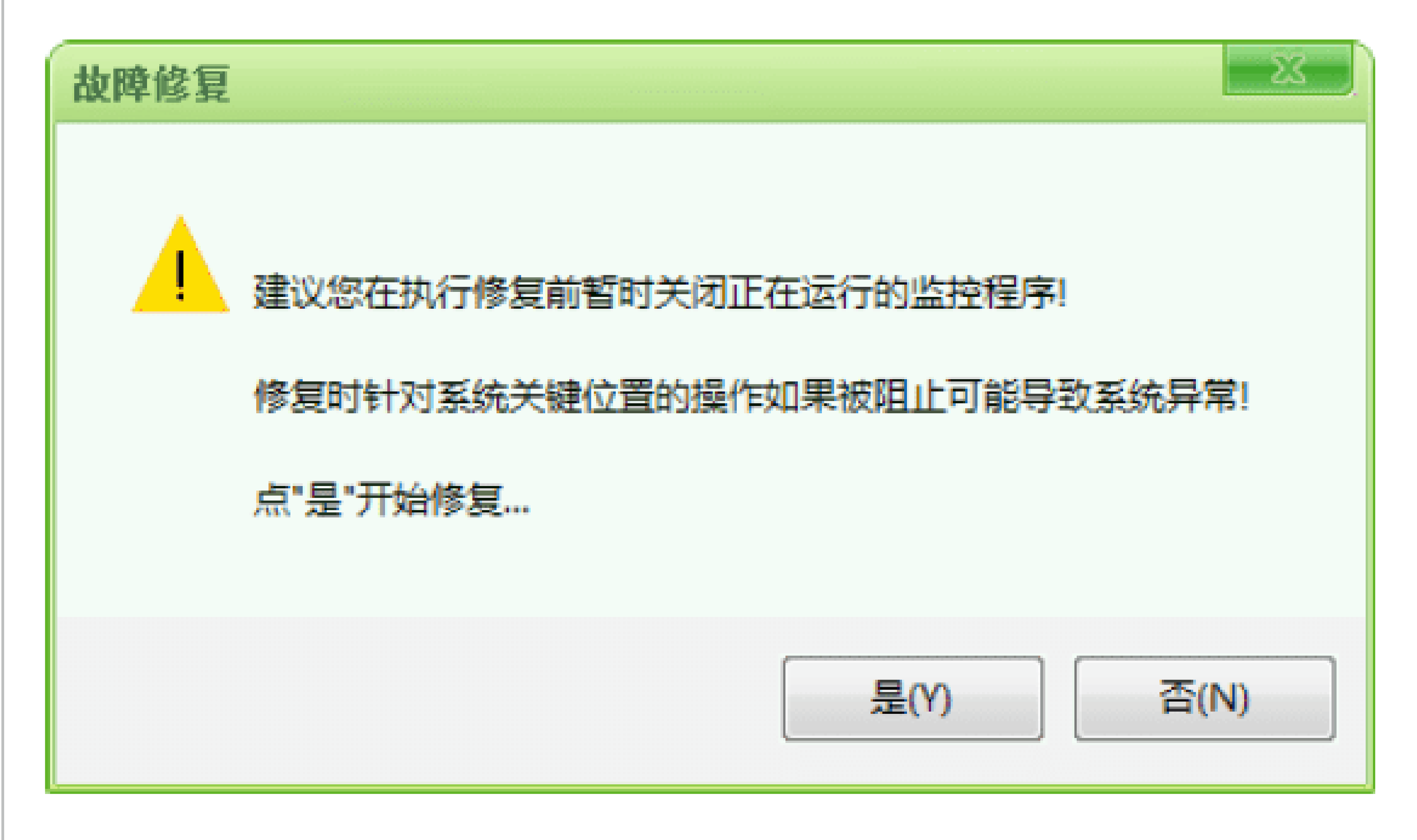
Step 08 单击“请点击此处，开始诊断”按钮，即可开始诊断系统，并在下方显示诊断的进度，如下图所示。



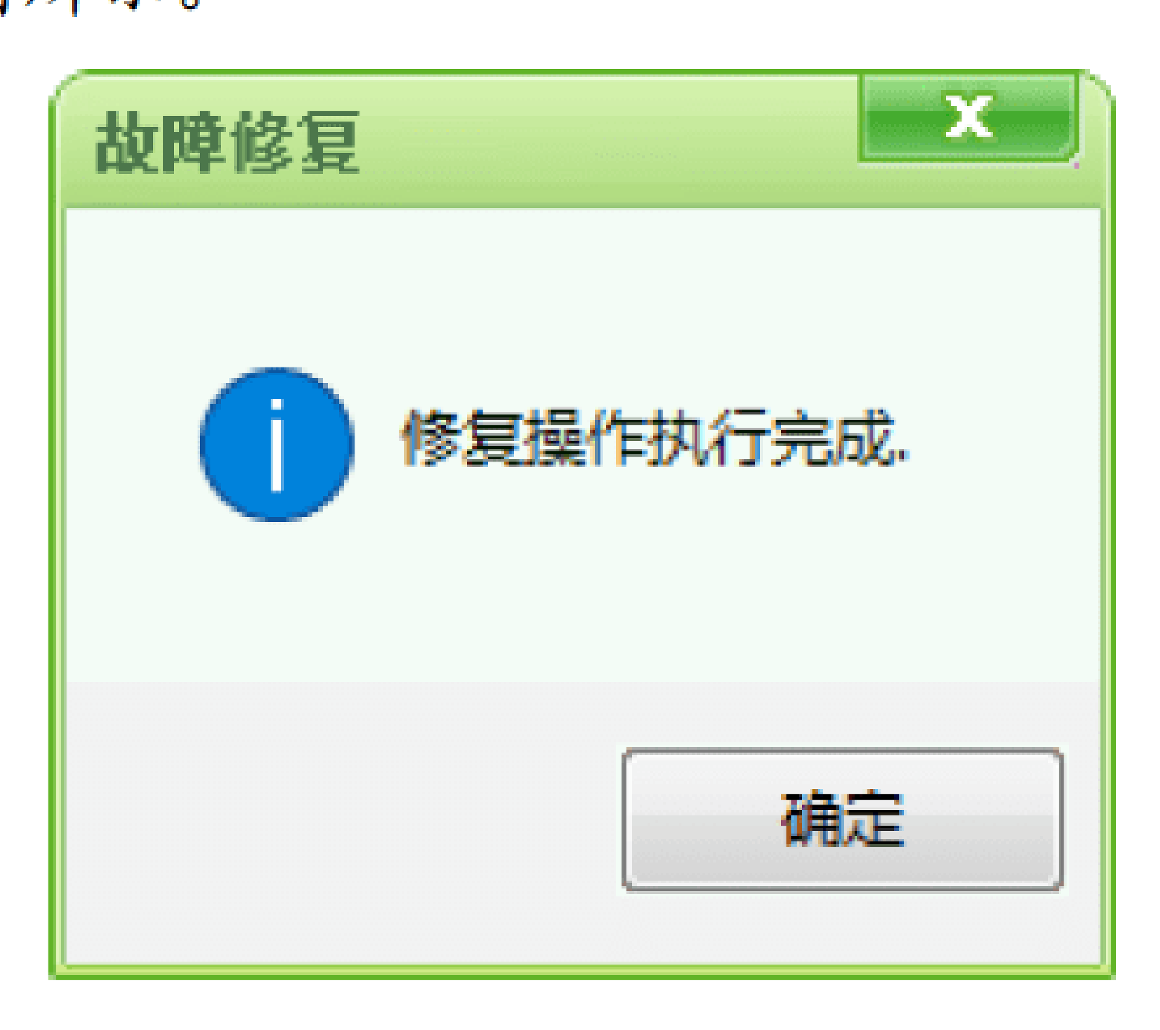
Step 09 选择“故障修复”选项，进入故障修复界面，在其中选择需要修复的对象，如下图所示。



Step 10 单击“执行修复”按钮，弹出“故障修复”对话框，提示用户修复前暂时关闭正在运行的监控程序，如下图所示。



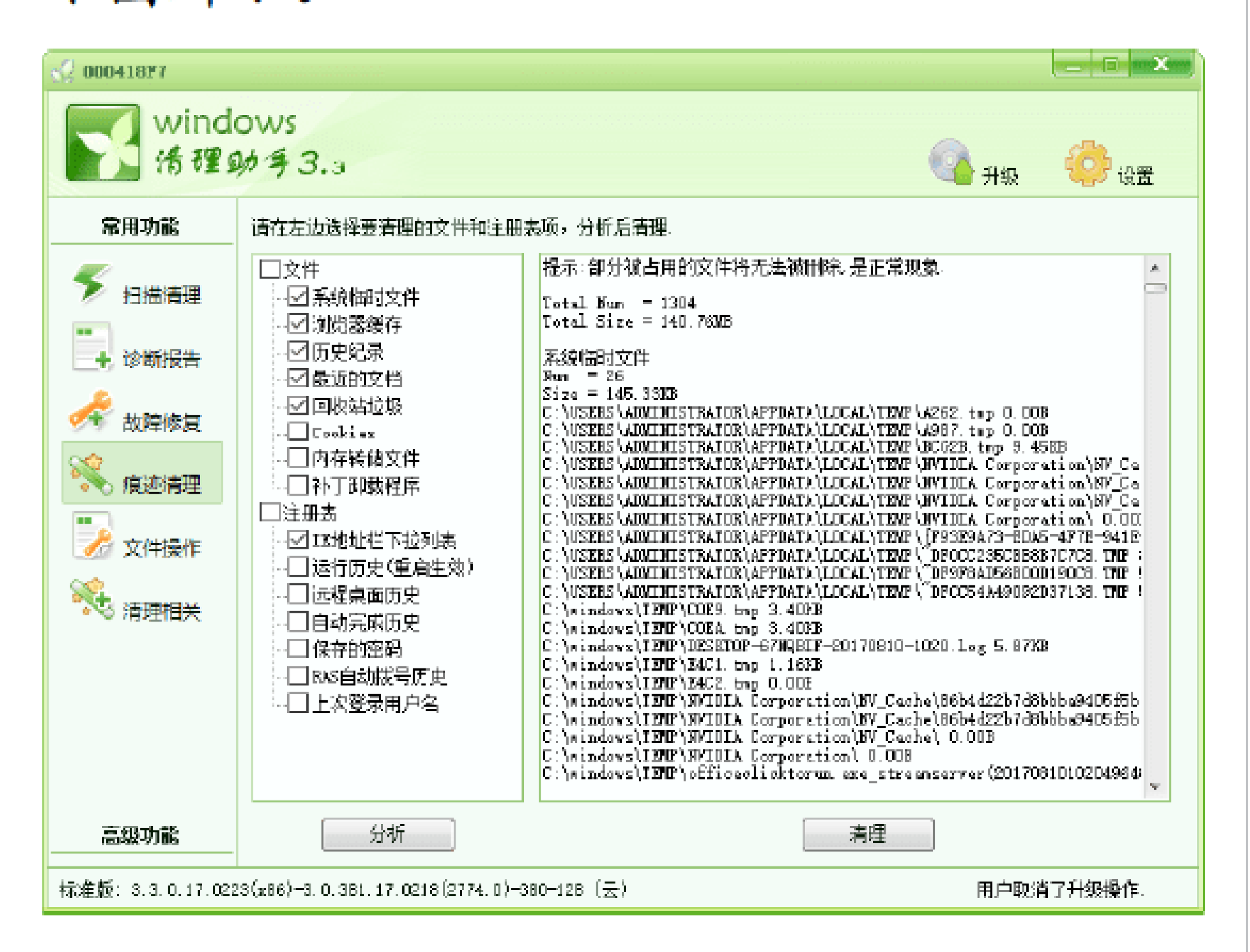
Step 11 单击“是”按钮，即可开始修复系统，修复完成后，弹出“故障修复”对话框，提示用户“修复操作执行完成”，如下图所示。



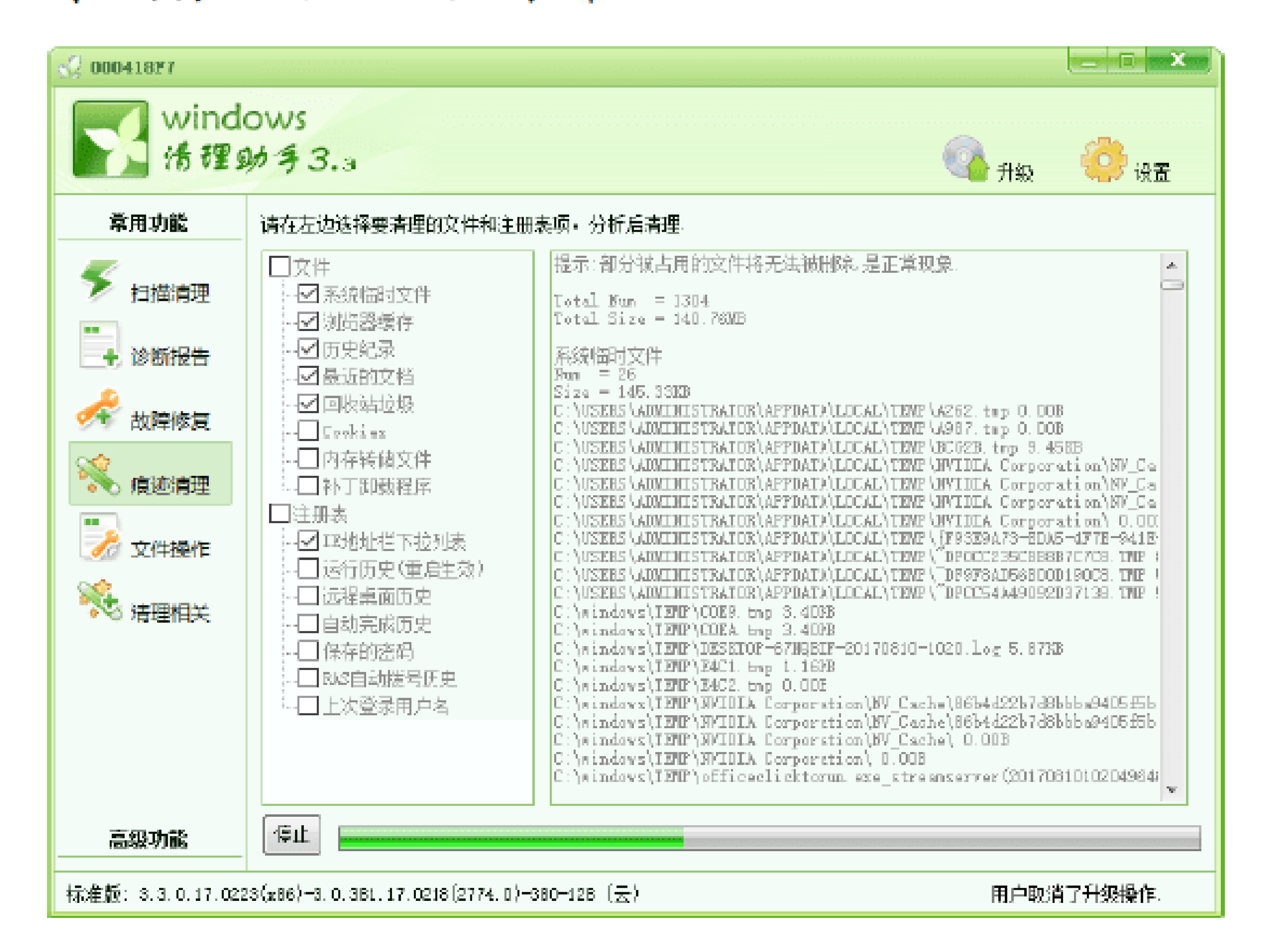
Step 12 选择“痕迹清理”选项，在打开的界面中选择要清理的文件和注册表项，如下图所示。



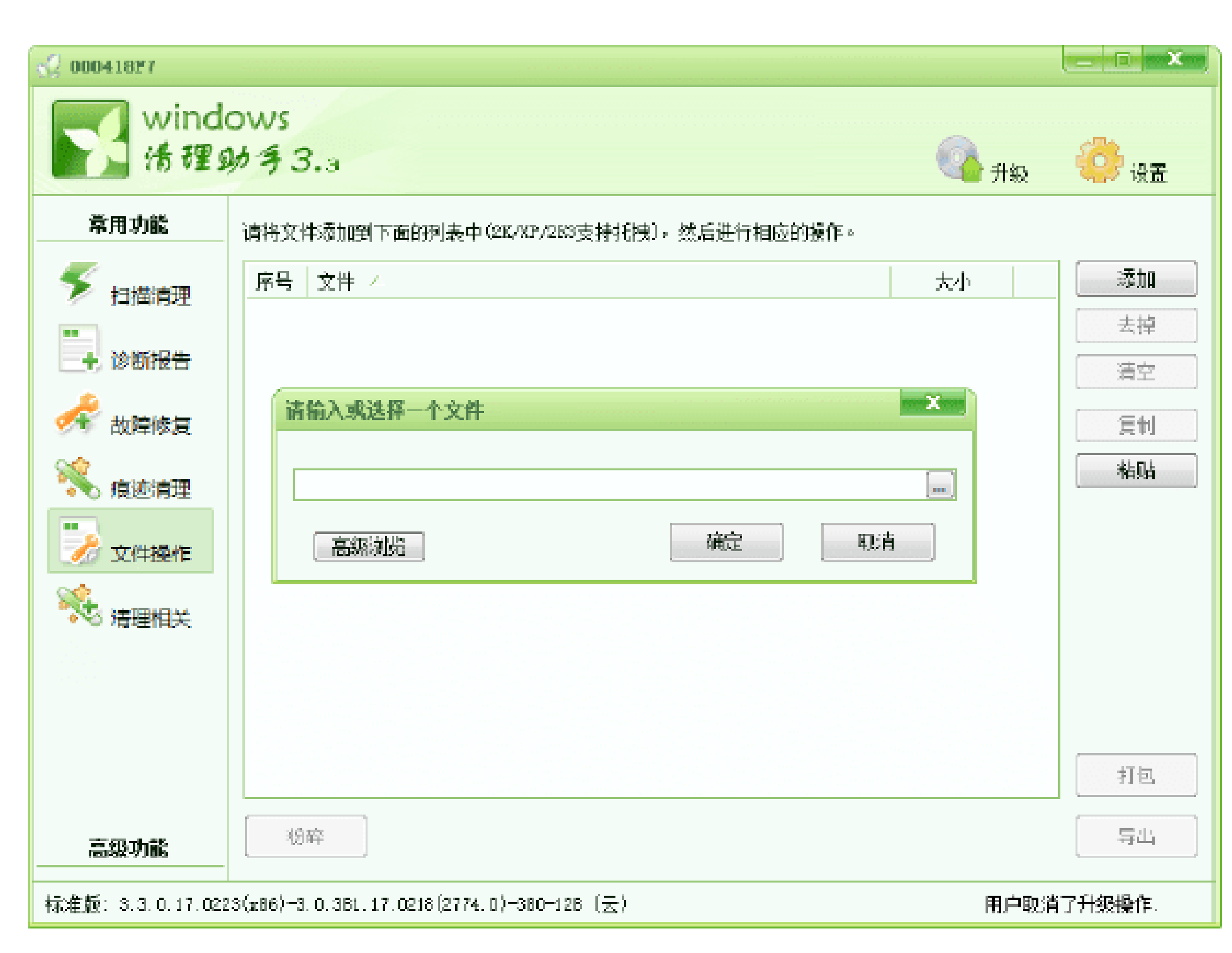
Step 13 单击“分析”按钮，即可开始分析痕迹，并在右侧的窗格中显示分析结果，如下图所示。



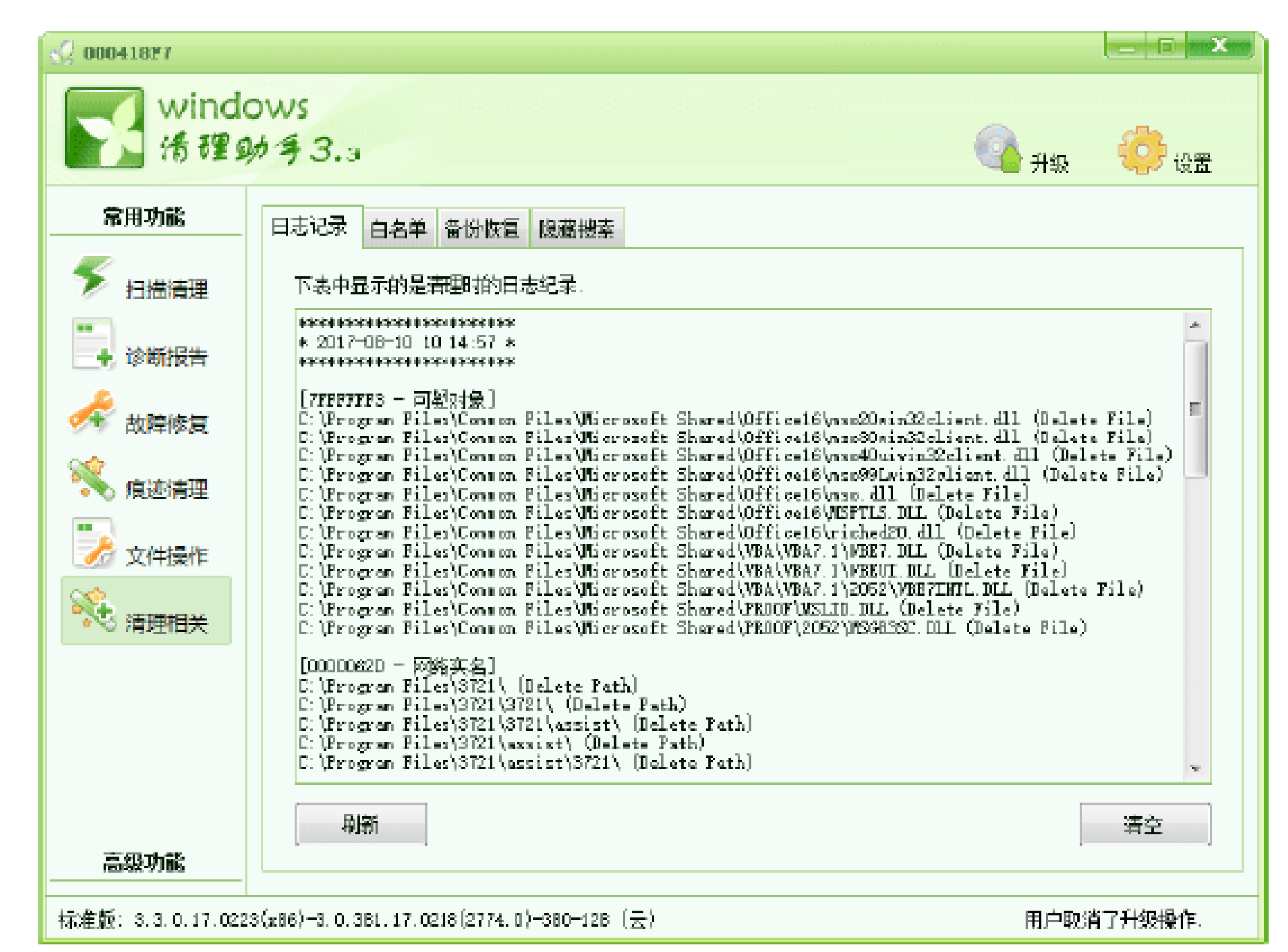
Step 14 单击“清理”按钮，即可清理扫描出来的痕迹，如下图所示。



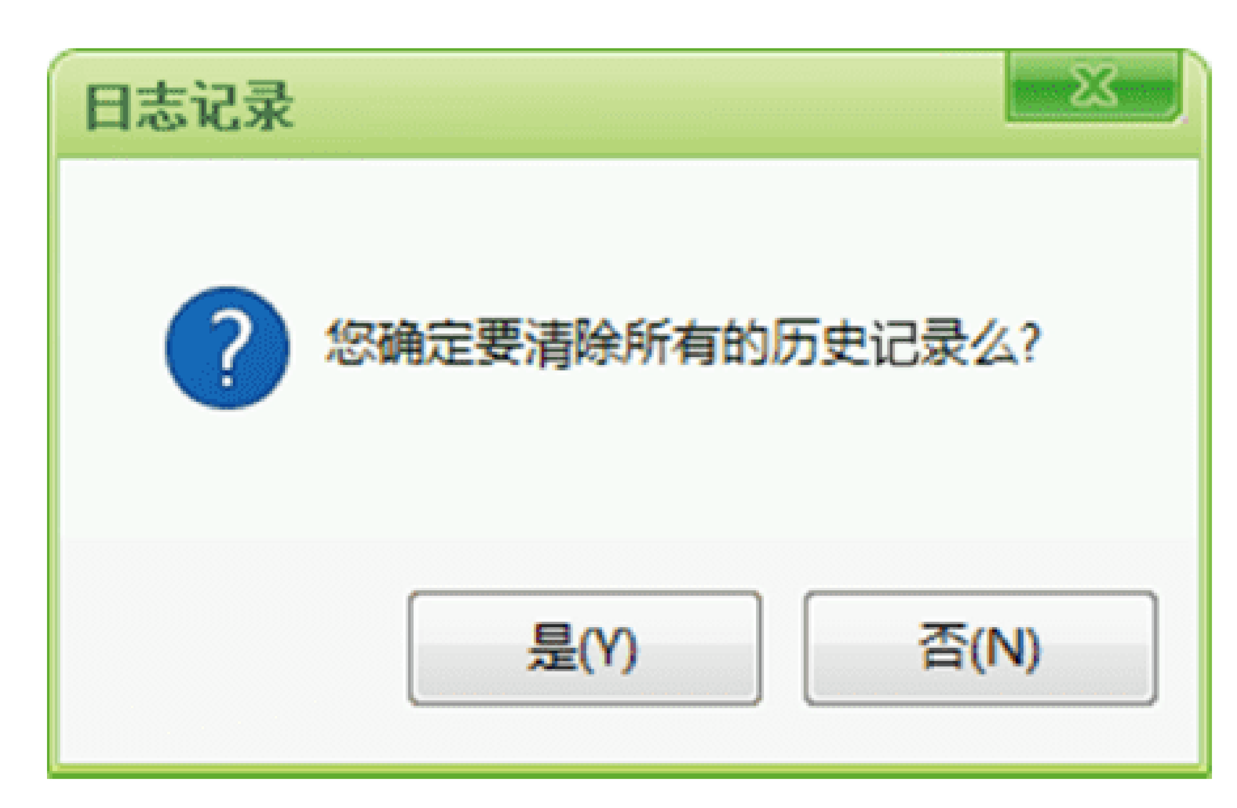
Step 15 选择“文件操作”选项，进入“文件操作”界面，通过单击“添加”按钮，可以添加相应的文件，如下图所示。



Step 16 选择“清理相关”选项，在打开的界面中可以查看清理时的日志记录，如下图所示。



Step 17 单击“清空”按钮，弹出“日志记录”对话框，提示用户是否确定要清除所有的历史记录，如下图所示，单击“是”按钮，即可清除所有的历史记录。



Step 18 选择“高级功能”选项，在弹出的列表中选择“脚本对象”选项，在其中可以启用“Windows清理助手”的脚本对象功能，如下图所示。



Step 19 选择“更多工具”选项，在打开的界面中可以查看“Windows 清理助手”提供的更多系统维护工具，如下图所示。

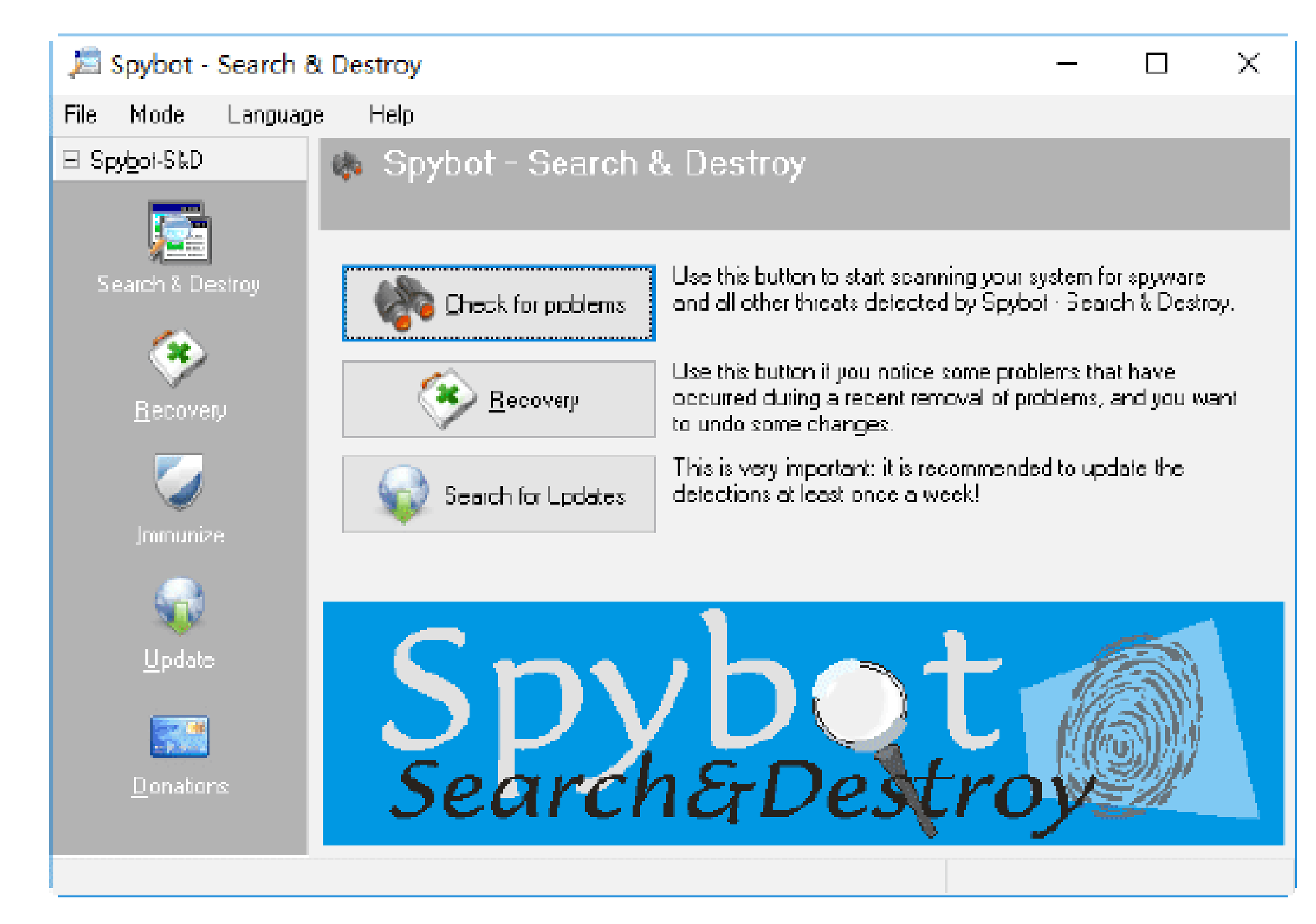


实战3：使用Spybot-Search&Destroy清理

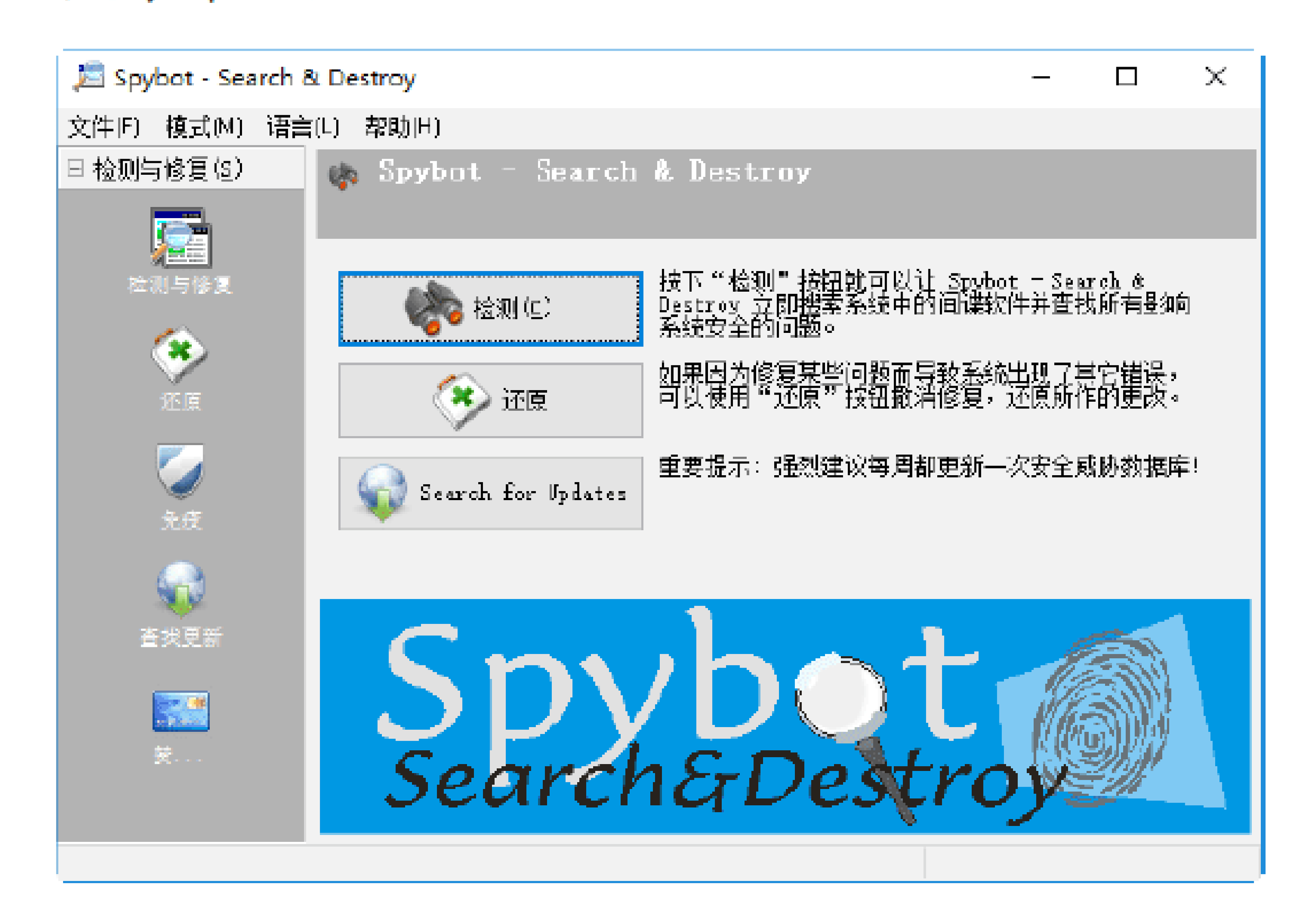
Spybot-Search&Destroy是一款专门用来清理间谍程序的工具。到目前为止，它已经可以检测一万多种间谍程序（Spyware），并对其中的一千多种进行免疫处理。同时这个软件是完全免费的，并有中文语言包支持，可以在Server级别的操作系统上使用。

下面介绍使用Spybot-Search&Destroy查杀间谍软件的基本步骤。

Step 01 安装Spybot-Search&Destroy，设置并初始化后，即可打开其主窗口，如下图所示。



Step 02 由于该软件支持多种语言，所以在其主窗口中选择Languages→“简体中文”选项，即可将程序主界面切换为中文模式，如下图所示。



Step 03 单击其中的“检测”按钮或单击左侧的“检查与修复”按钮，即可打开“检测与修复”窗口，如下图所示，单击“检测与修复”按钮，即可开始检查系统中存在的间谍软件。

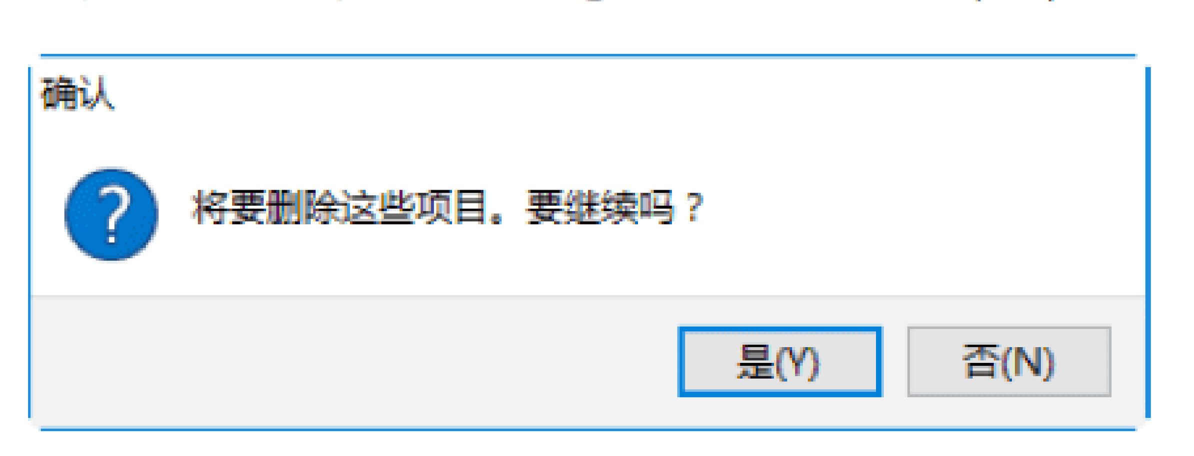


Step 04 在软件检查完毕之后，检查页上将会列出在系统中查到可能有问题的软件。选取某个检查到的问题，再单击右侧的分栏箭头，即可查询到有关该问题软件的发布公

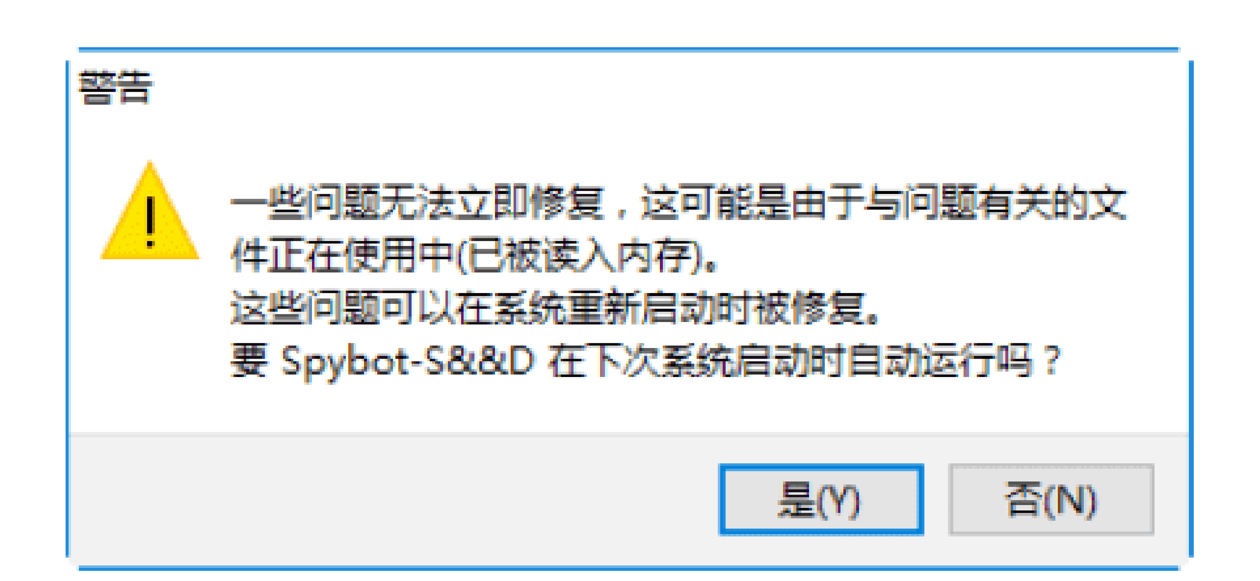
司、软件功能、说明和危害种类等信息，如下图所示。



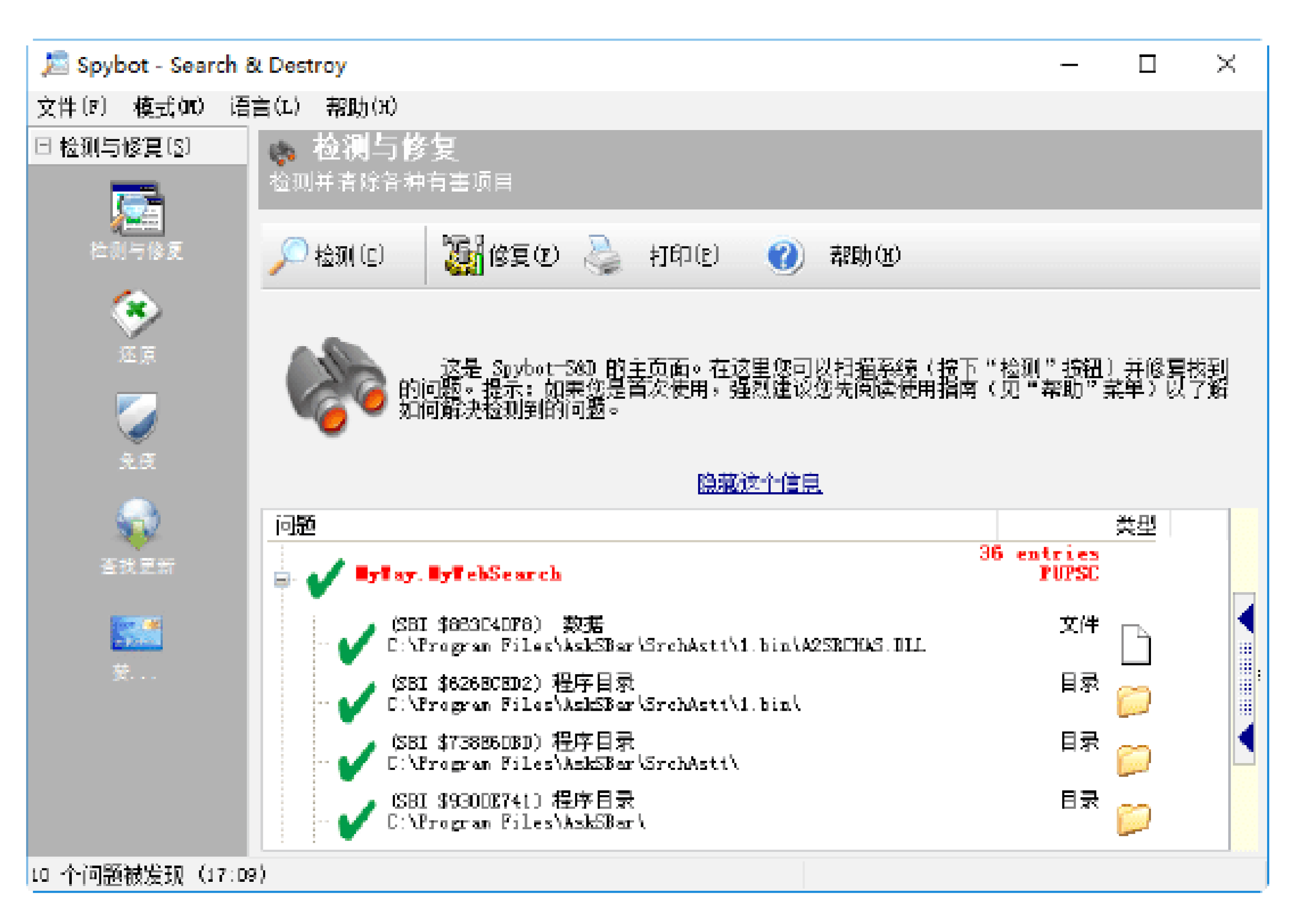
Step 05 选中需要修复的问题程序，单击“修复”按钮，即可打开“将要删除这些项目。要继续吗？”提示信息框，如下图所示。



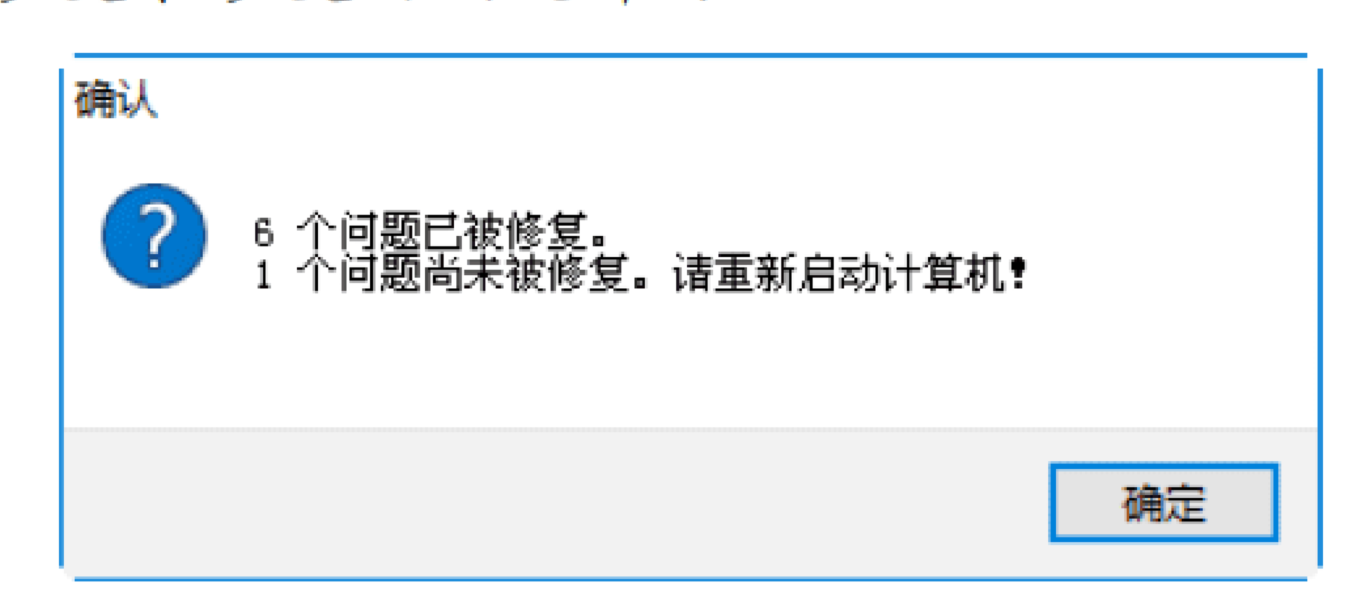
Step 06 单击“是”按钮，即可看到“在下次系统启动时自动运行吗？”提示框，如下图所示。



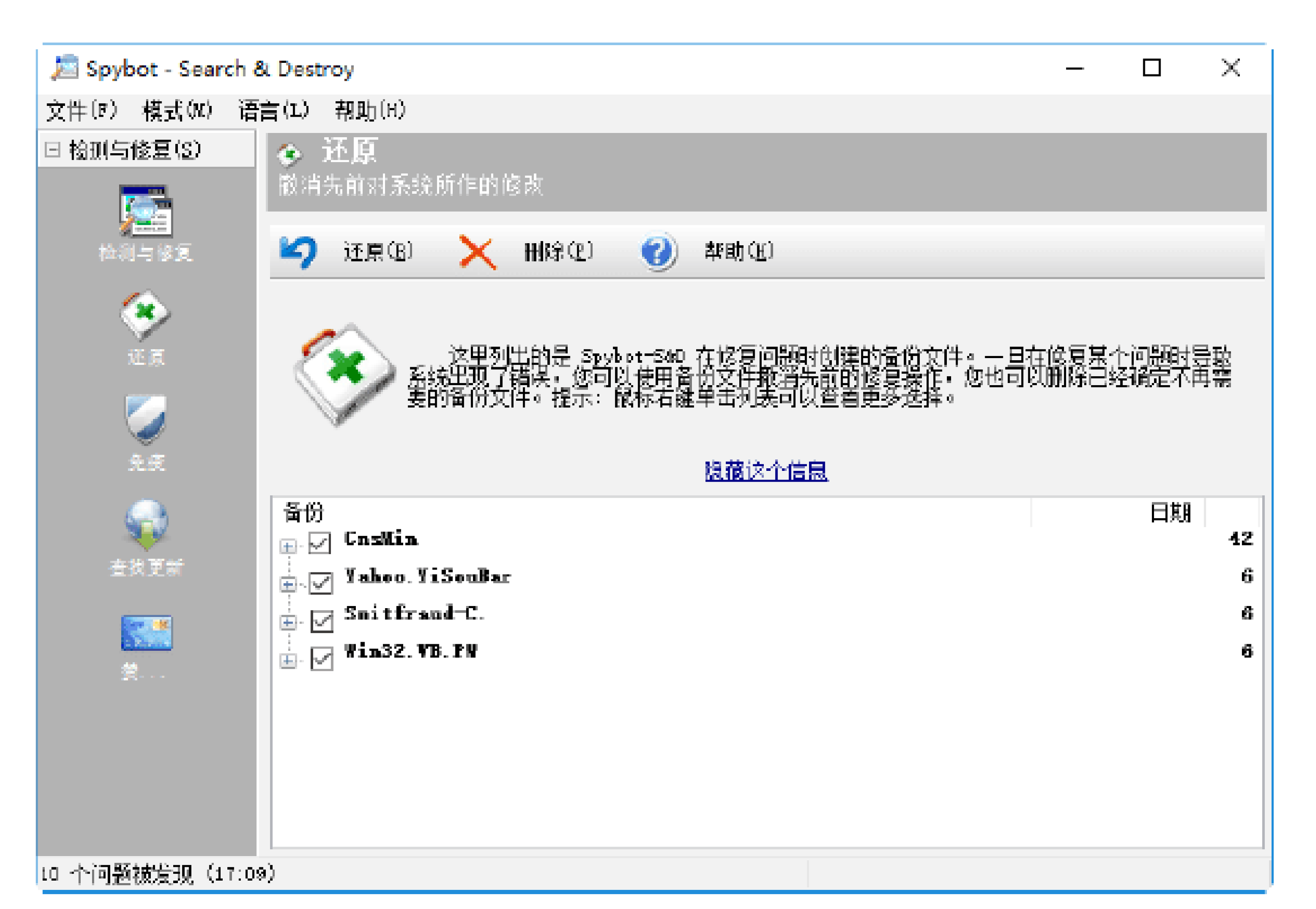
Step 07 单击“是”按钮，即可将选取的间谍程序从系统中清除。修复后的结果如下图所示，其中用✔标识已经成功修复的问题，用✖标识修复不成功的问题。



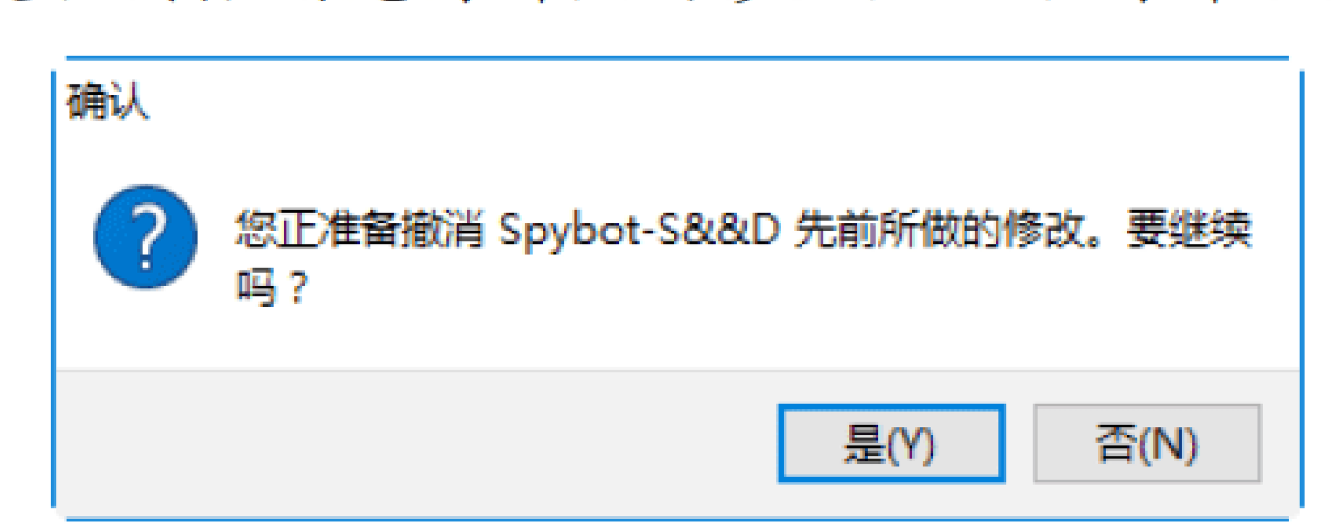
Step 08 待修复完成后，即可看到“确认”对话框。在其中会显示成功修复以及尚未修复问题的数目，并建议重启计算机，如下图所示。单击“确定”按钮，重启计算机修复未修复的问题即可。



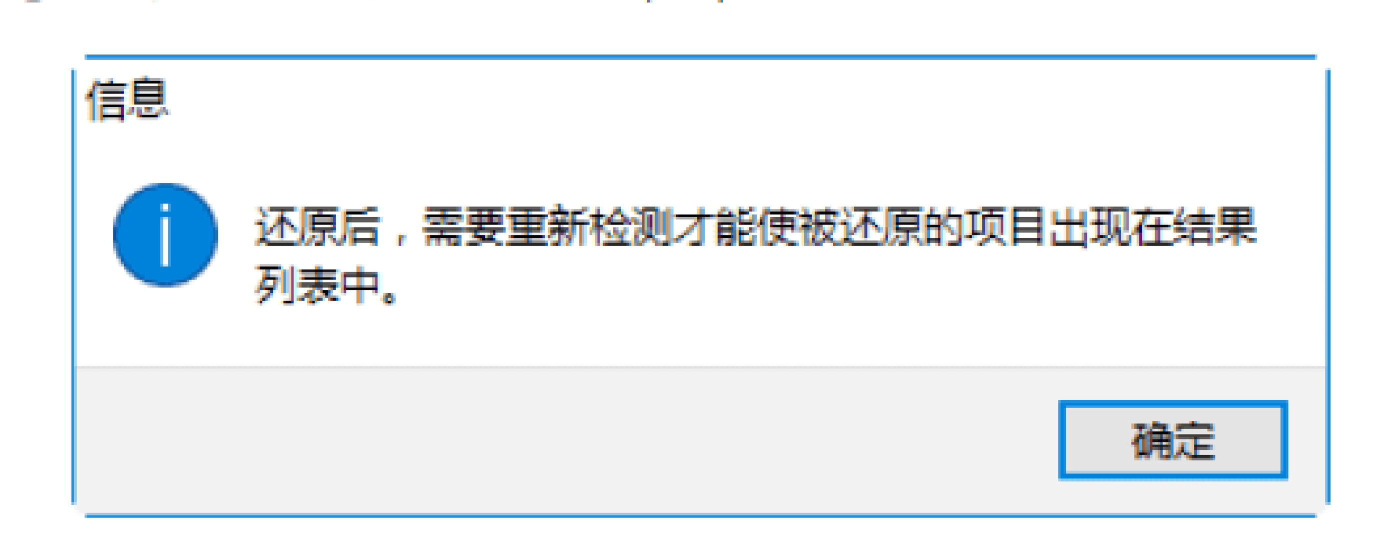
Step 09 选择“还原”选项，在打开的界面中选择需要还原的项目，单击“还原”按钮，如下图所示。



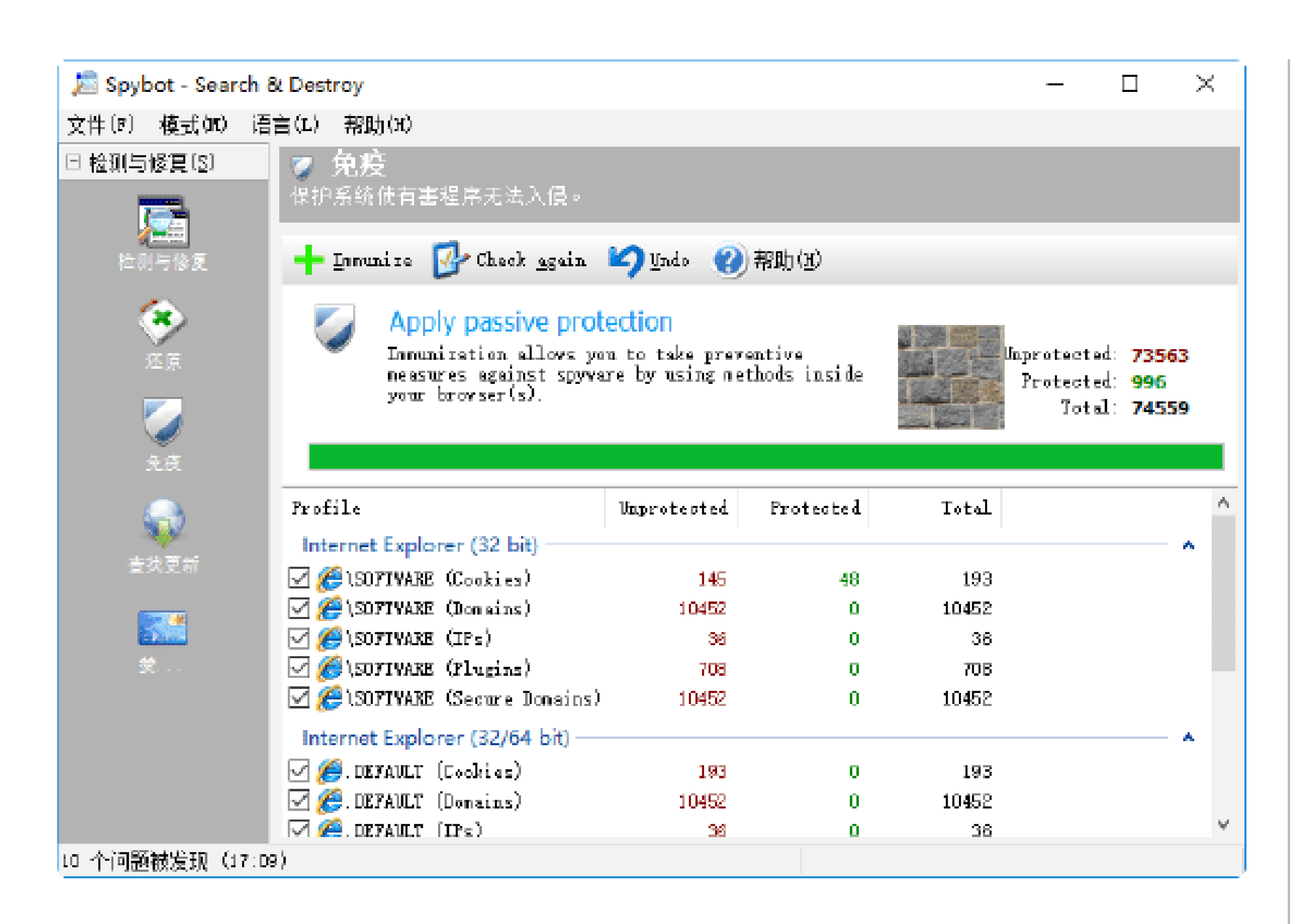
Step 10 弹出“确认”信息提示框，提示用户是否要撤销先前所做的修改，如下图所示。



Step 11 单击“是”按钮，即可将修复的问题还原到原来的状态，还原完毕后弹出“信息”提示框，如下图所示。



Step 12 选择“免疫”选项，进入“免疫”设置界面，如下图所示，免疫功能能使用户的系统具有抵御间谍软件的免疫效果。



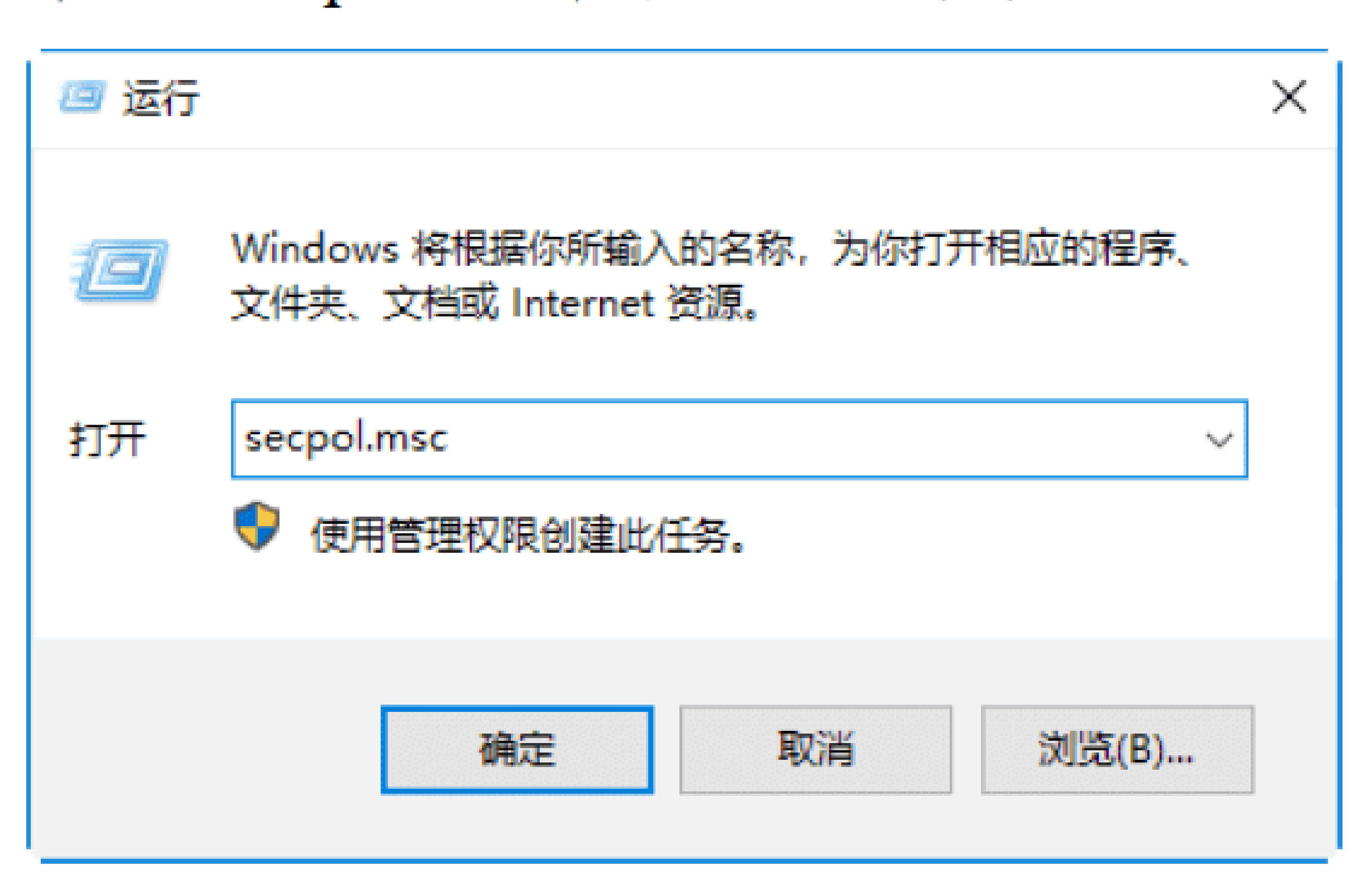
13.2 通过本地安全设置保护系统安全

Windows 10系统自带的“本地安全策略”是一个很不错的系统安全管理工具，利用它可以使自己的操作系统更加安全。下面将具体讲解设置本地安全策略的各种方法。

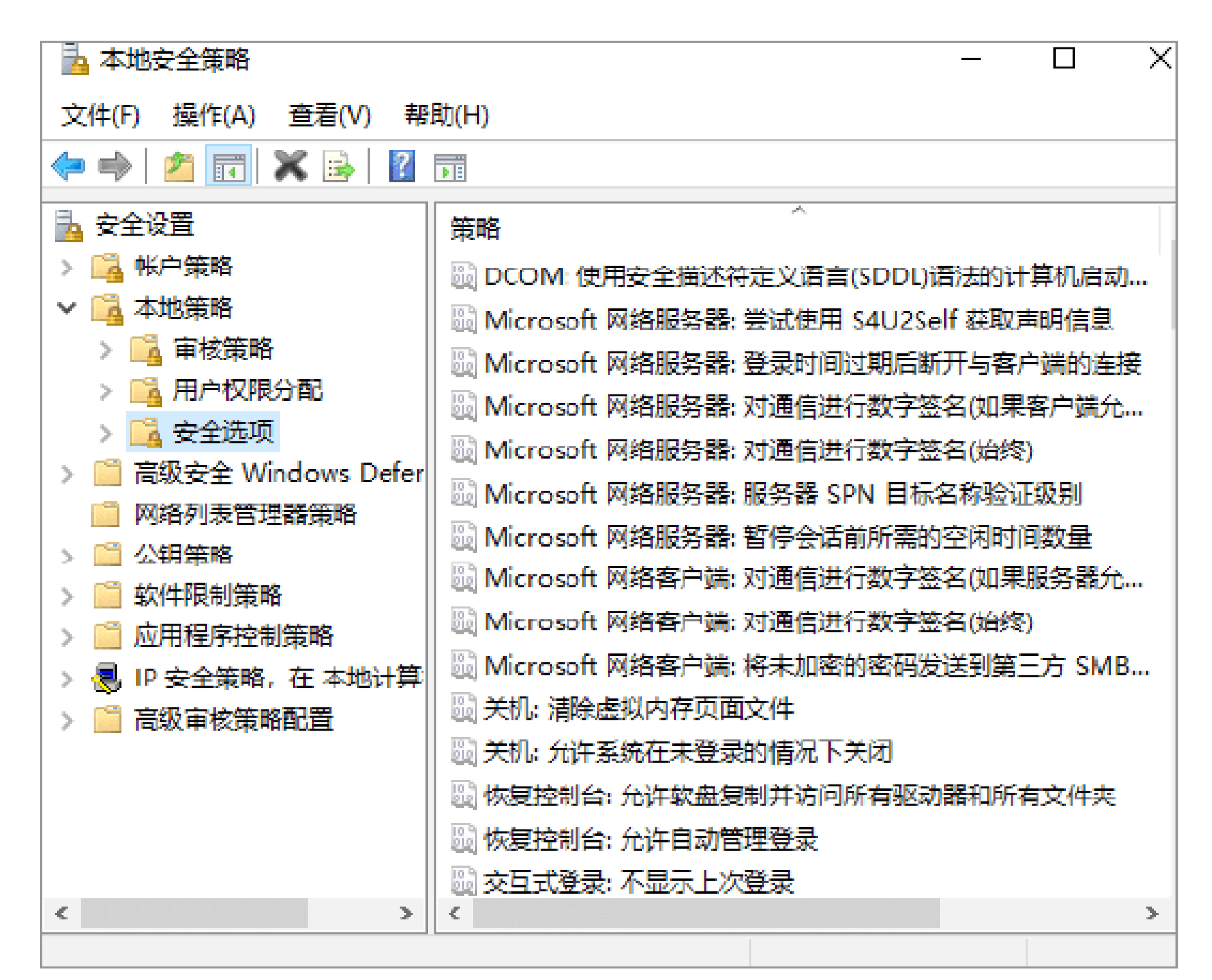
实战4：禁止在登录前关机

在工作中如果需要暂时离开，可以按WIN+L组合键来锁定计算机，回来后只需输入登录密码即可继续工作。但在锁定界面中有一个“关闭计算机”选项，为了防止他人关闭计算机，可以通过启用“禁止在登录前关机”安全策略来实现。

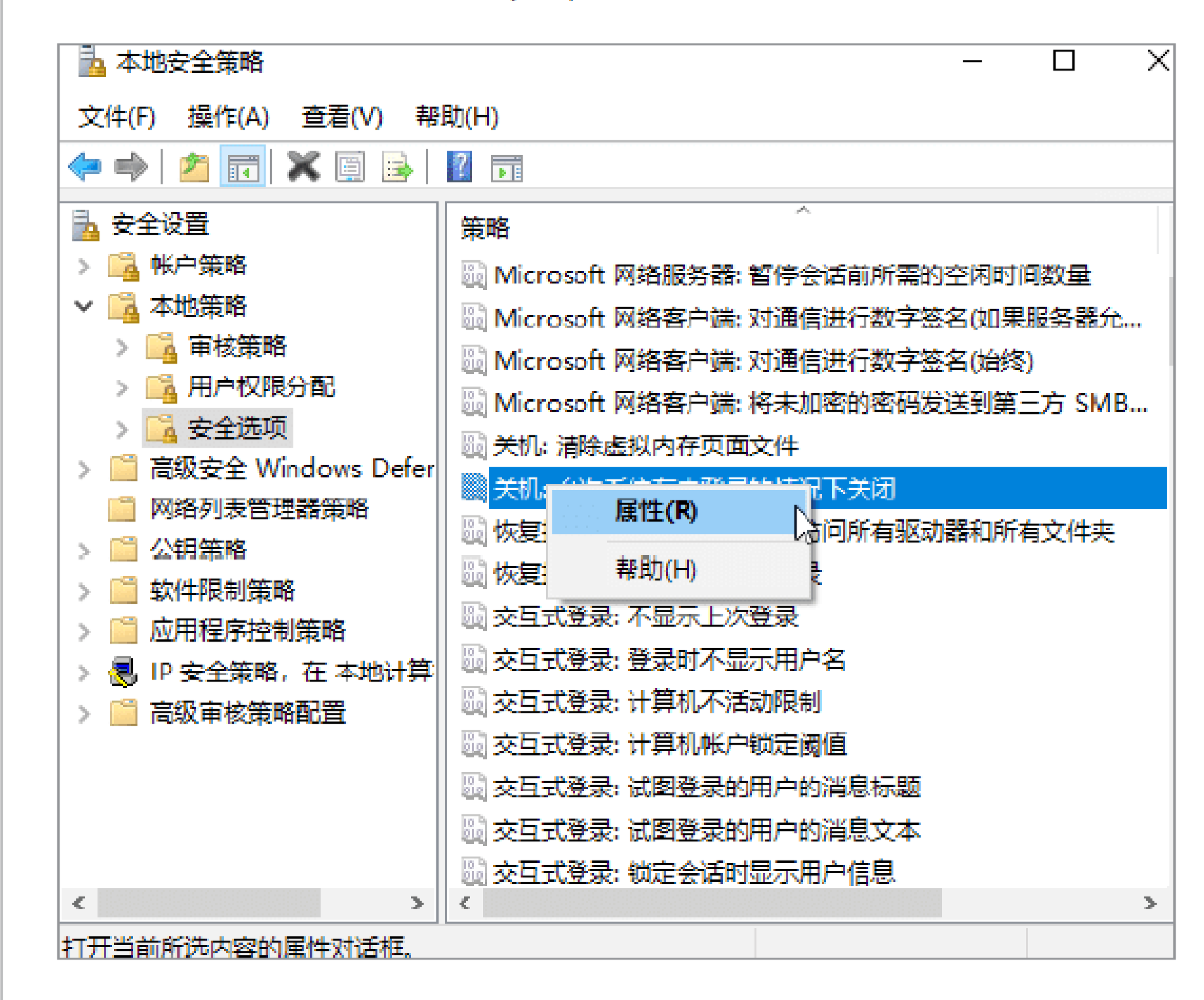
Step 01 单击“开始”→“运行”命令，打开“运行”对话框，然后在“打开”文本框中输入secpol.msc命令，如下图所示。



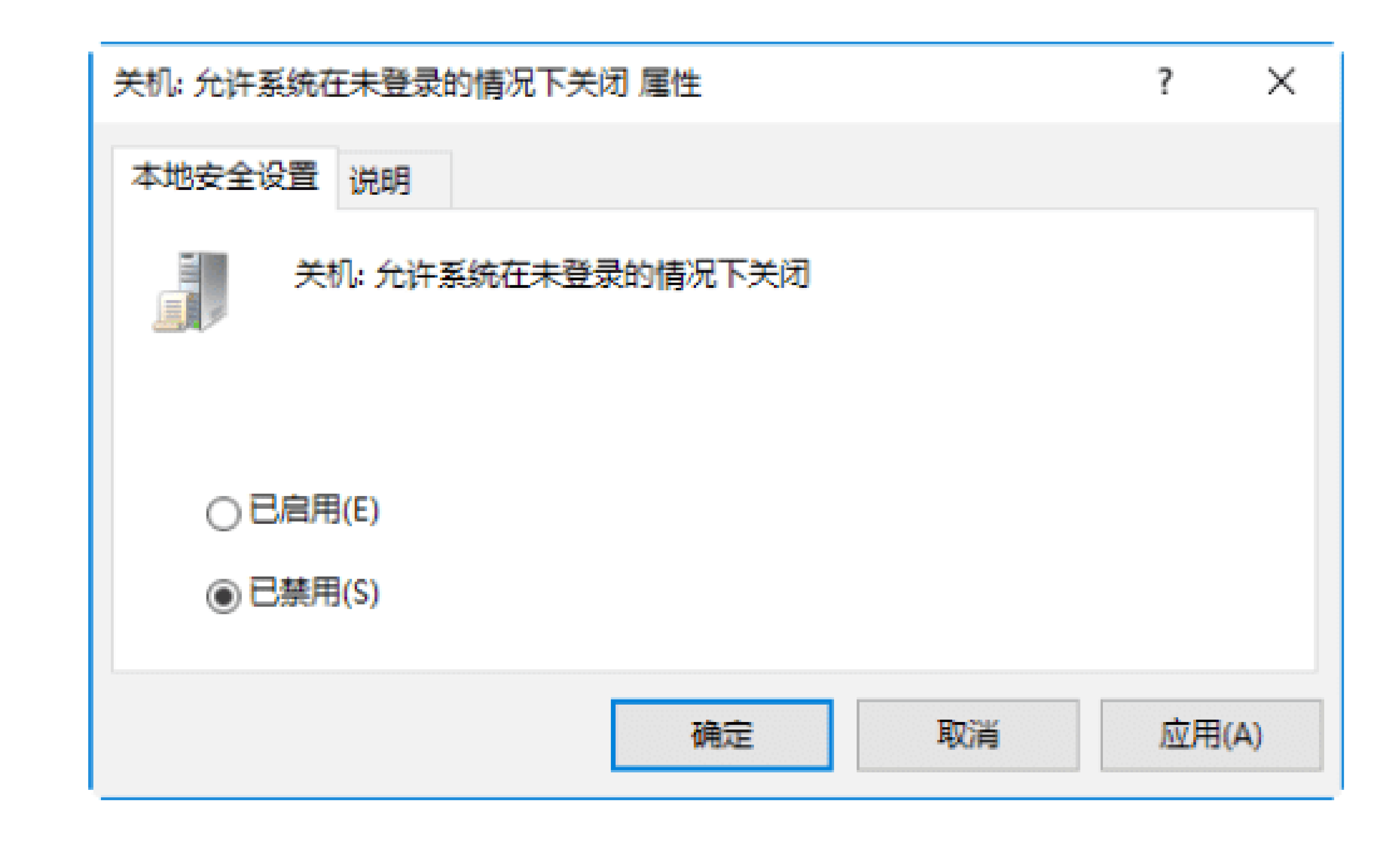
Step 02 单击“确定”按钮，打开“本地安全策略”窗口，然后在左侧窗格中依次展开“安全设置”→“本地策略”→“安全选项”选项，如下图所示。



Step 03 在右侧窗格中找到“关机：允许系统在未登录的情况下关闭”选项，在该选项上右击，在弹出的快捷菜单中选择“属性”选项，如下图所示。



Step 04 打开“关机：允许系统在未登录的情况下关闭 属性”对话框，在该对话框中选中“已禁用”单选按钮，如下图所示，然后依次单击“应用”和“确定”按钮，即可完成设置。

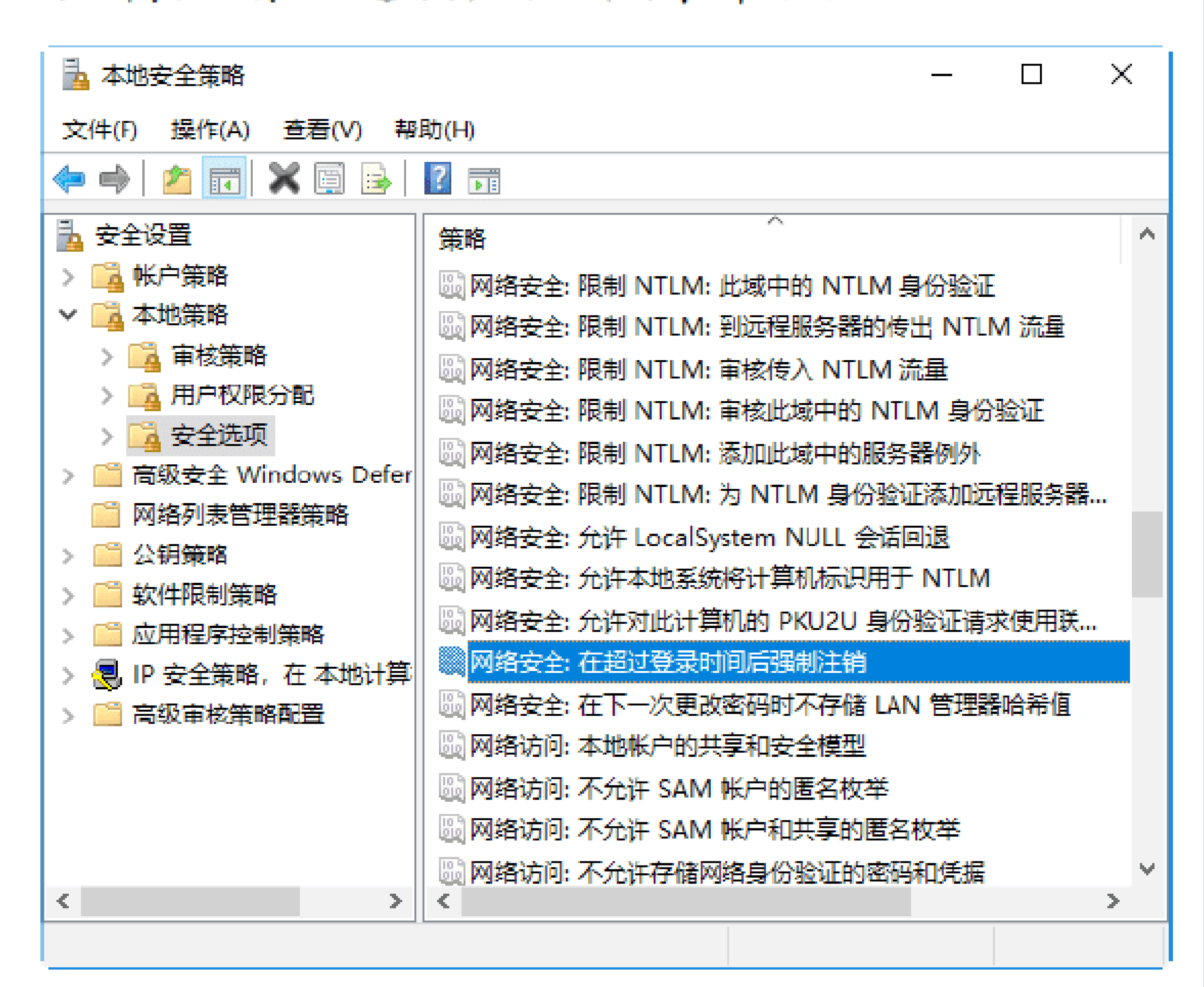


提示：“禁止在登录前关机”安全策略选项用来确定是否可以在无须登录到Windows的情况下关闭计算机。禁用此策略时，Windows登录屏幕上的“关机”命令可用。启用此策略时，Windows登录屏幕上不会显示“关闭计算机”选项。在这种情况下，用户必须能够成功登录到计算机并具有关闭系统的用户权限，然后才可以执行系统关闭操作。

实战5：在超过登录时间后强制用户注销

当某些用户连接到本地计算机上且已经超过有效登录时间时，需要让计算机自动断开与该用户的连接，利用“网络安全：在超过登录时间后强制注销”选项可以解决这一问题。具体的操作步骤如下。

Step 01 打开“本地安全策略”窗口，在左侧窗格中依次展开“安全设置”→“本地策略”→“安全选项”选项，然后在右侧窗格中找到“网络安全：在超过登录时间后强制注销”选项，如下图所示。



Step 02 双击该选项，打开“网络安全：在超过登录时间后强制注销 属性”对话框，选中“已启用”单选按钮，如下图所示，然后依次单击“应用”和“确定”按钮，即可应用设置。



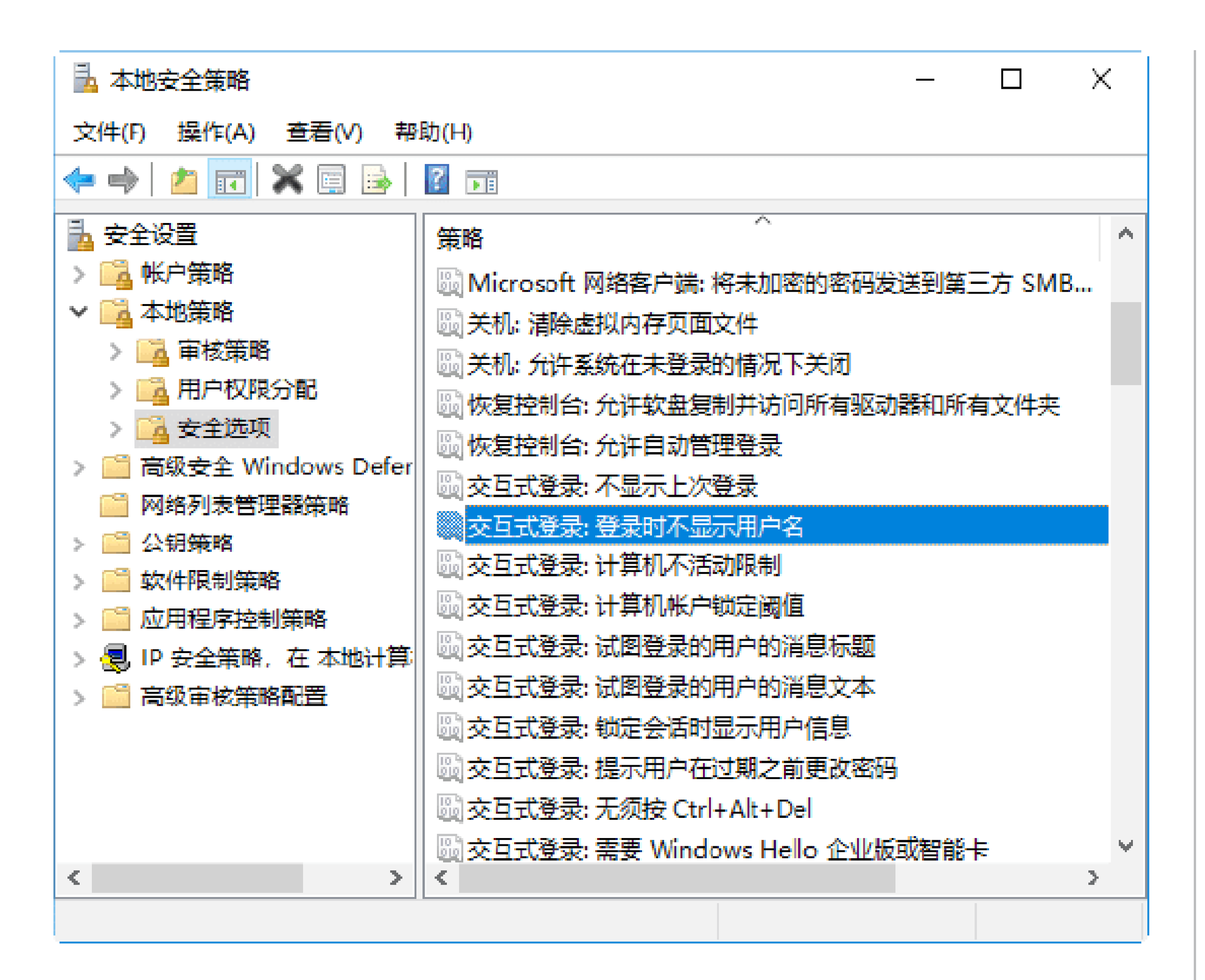


提示：“网络安全：在超过登录时间后强制注销”安全策略选项用于确定在连接到本地计算机的用户超出其用户账户的有效登录时间时，是否断开与其的连接，此设置会影响服务器消息块（SMB）组件。启用此策略时，一旦客户端的登录时间过期，该策略便会强制断开与SMB服务器建立的客户端会话。如果禁用此策略，即便在客户端登录时间过期后，仍允许维持已建立的客户端会话。

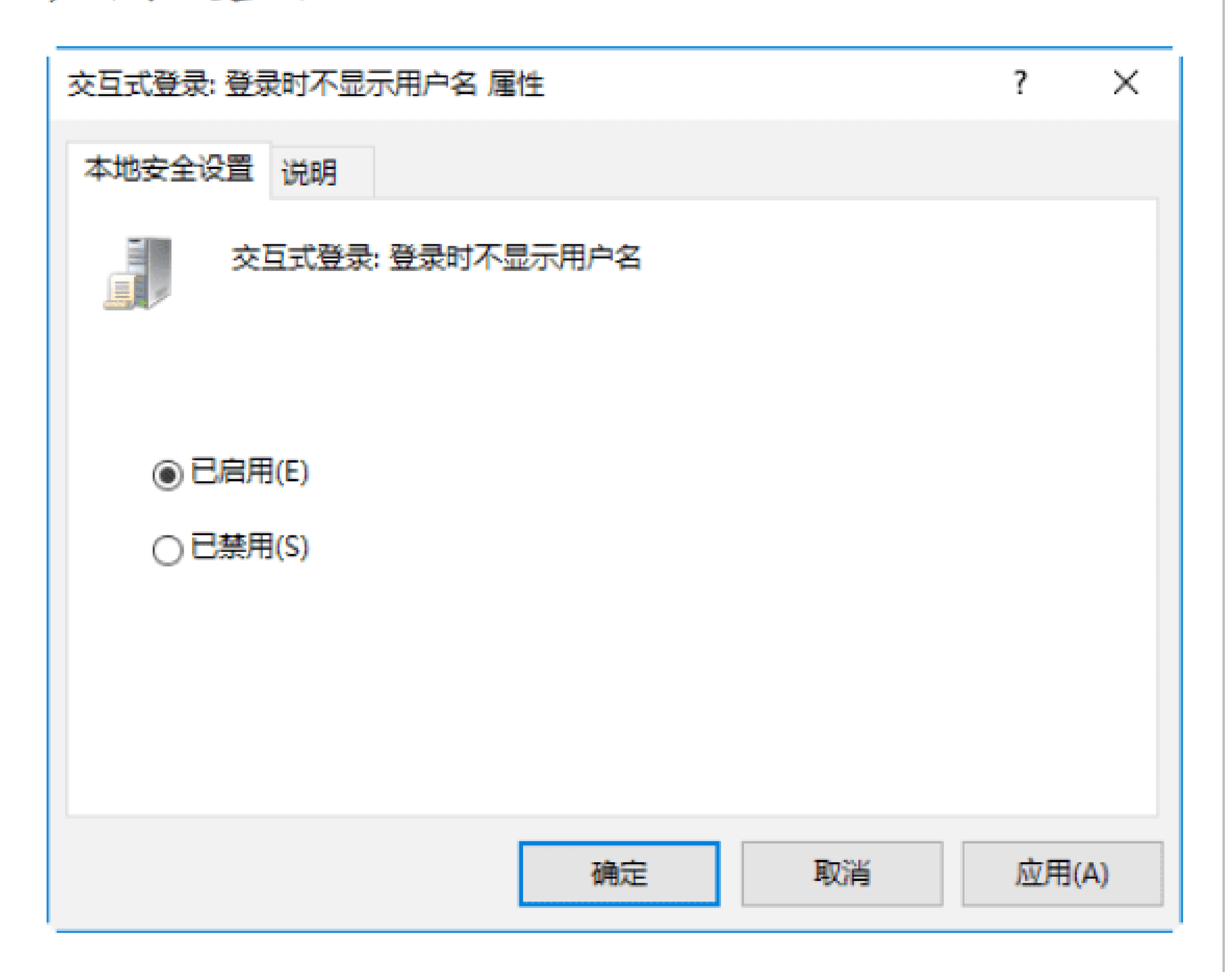
实战6：登录时不显示用户名

在登录计算机系统时，上次成功登录的用户名会显示在Windows登录界面上，这可能造成账户信息的泄露，给黑客以可乘之机。为了让最后成功登录的用户名在登录界面不再显示，可以通过启用“交互式登录：登录时不显示用户名”安全策略来实现。具体操作步骤如下。

Step 01 打开“本地安全策略”窗口，在左侧窗格中依次展开“安全设置”→“本地策略”→“安全选项”选项，然后在右侧窗格中找到“交互式登录：登录时不显示用户名”选项，如下图所示。



Step 02 双击该选项，打开“交互式登录：登录时不显示用户名 属性”对话框，选中“已启用”单选按钮，如下图所示，然后依次单击“应用”和“确定”按钮，即可应用设置。



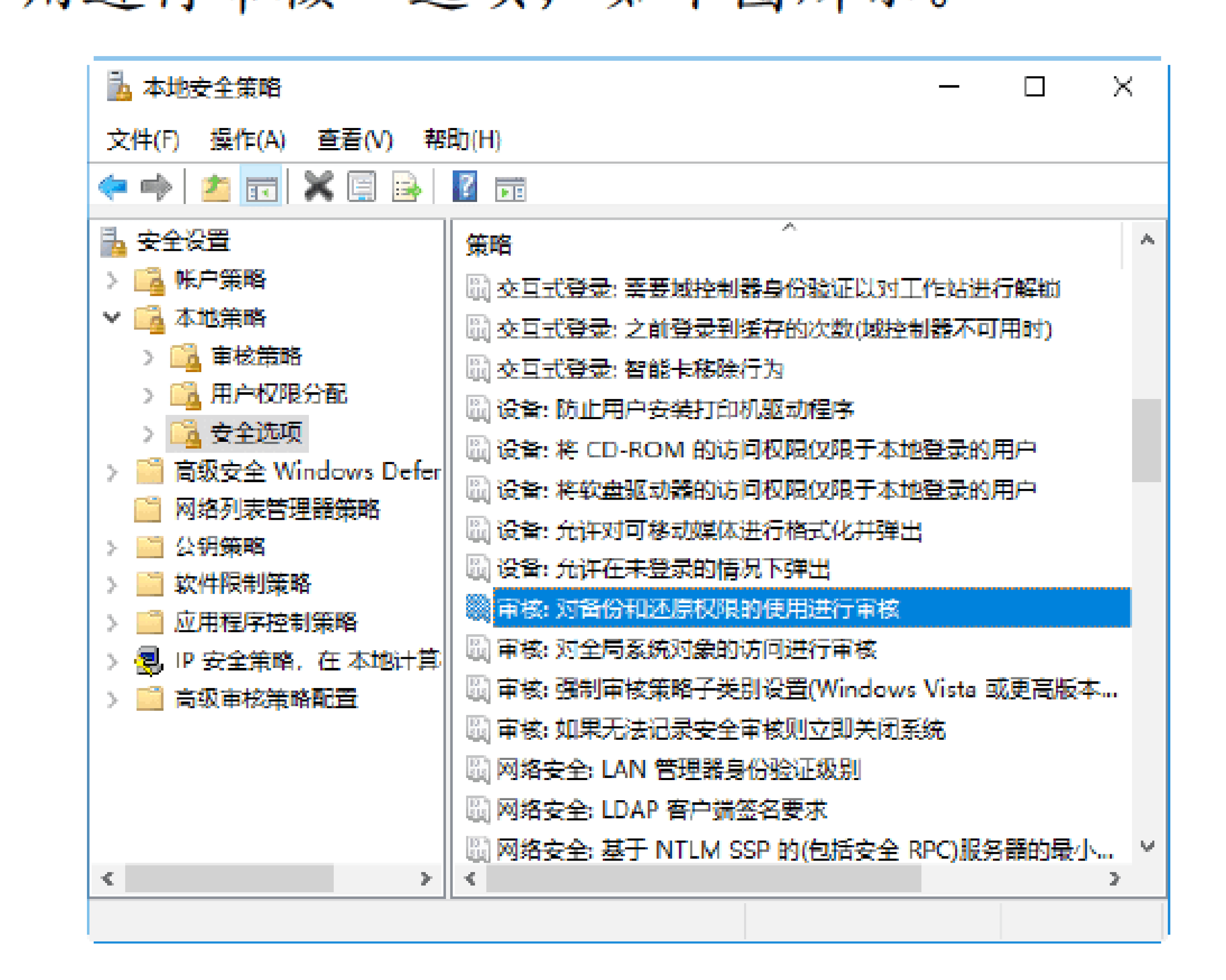
提示：“交互式登录：登录时不显示用户名”安全策略选项用于确定是否在Windows登录屏幕中显示最后登录到计算机的用户的名称。如果启用该策略，则不会在“登录到Windows”对话框中显示最后成功登录的用户名；如果禁用该策略，则会显示最后登录的用户名。



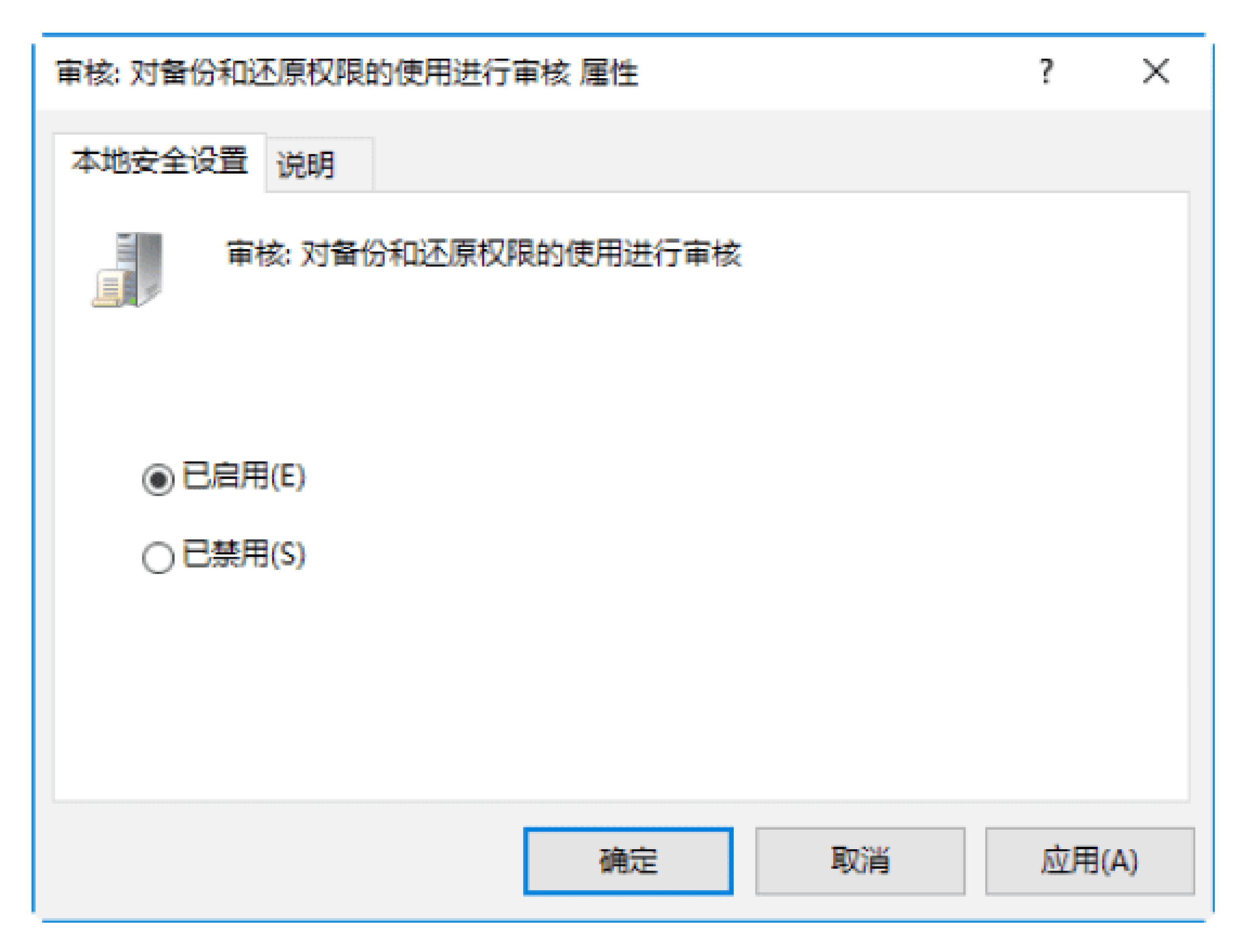
实战7：对备份和还原权限进行审核

启用对备份和还原权限的使用进行审核功能，可以将所有实施用户权限的实例都记录到安全日志中，用户可以通过在“本地安全策略”窗口中启用“审核：对备份和还原权限的使用进行审核”安全策略来实现。具体操作步骤如下。

Step 01 打开“本地安全策略”窗口，在左侧窗格中依次展开“安全设置”→“本地策略”→“安全选项”选项，然后在右侧窗格中找到“审核：对备份和还原权限的使用进行审核”选项，如下图所示。



Step 02 双击该选项，打开“审核：对备份和还原权限的使用进行审核 属性”对话框，选中“已启用”单选按钮，如下图所示，然后依次单击“应用”和“确定”按钮，即可应用设置。

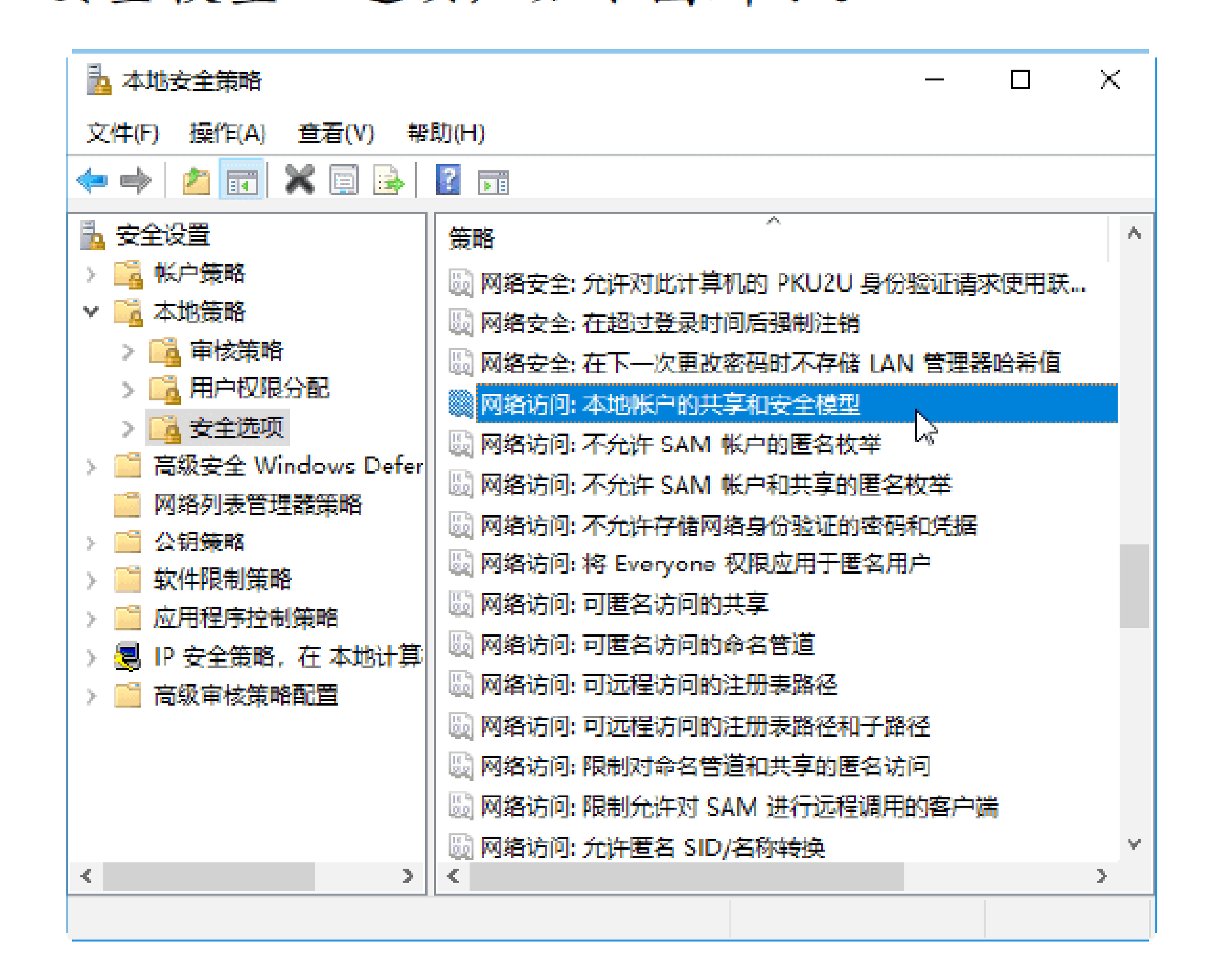


提示：“审核：对备份和还原权限的使用进行审核”安全策略选项用于确定当审核权限使用策略生效时，是否审核包括备份和还原在内的所有用户权限的使用。启用审核权限使用策略的同时启用此选项，会为备份或还原的每个文件生成一个审核事件。如果禁用此策略，则即使启用了审核权限使用，也不会审核备份或还原权限的使用。

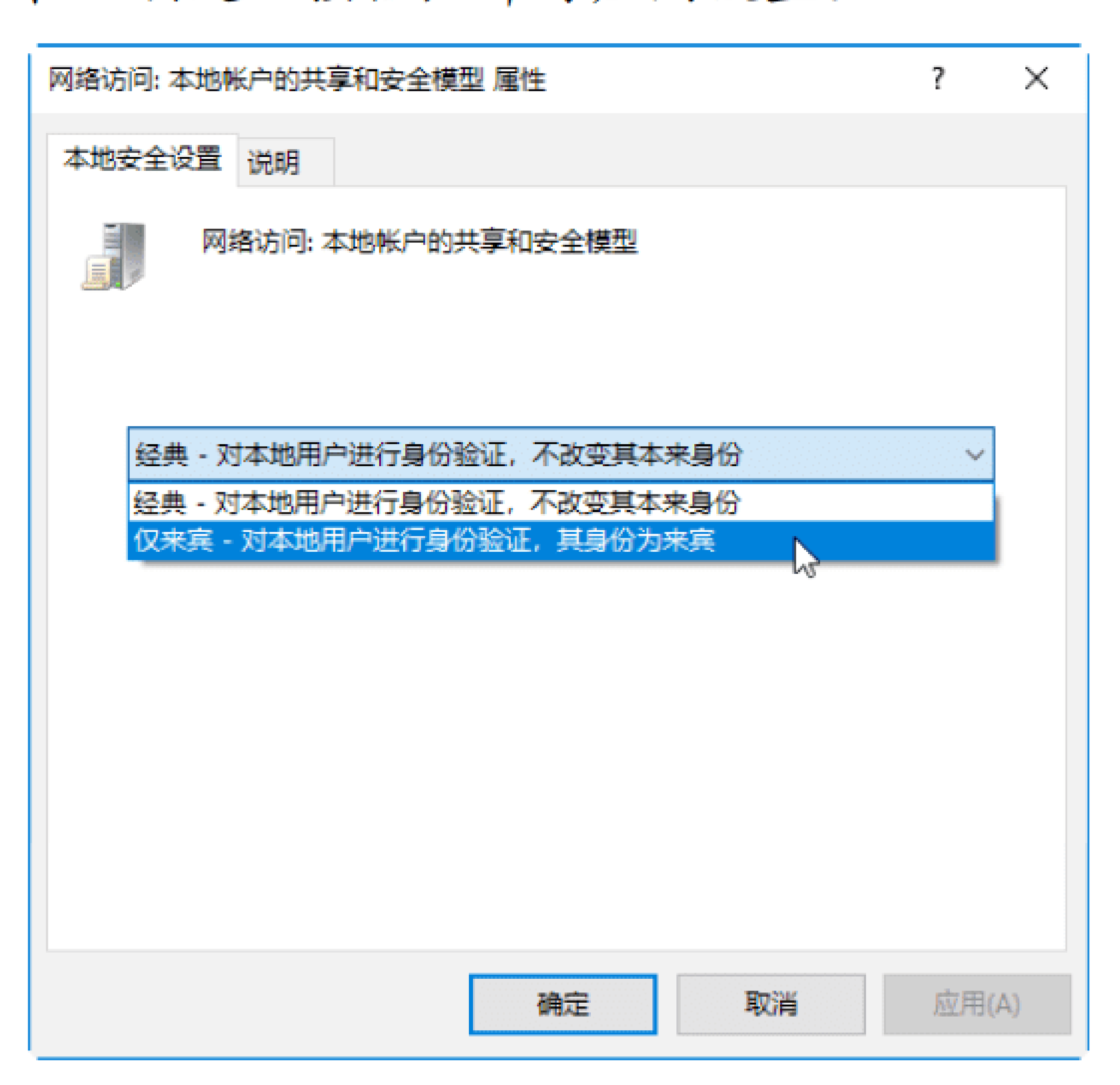
实战8：设置本地账户共享与安全模式

在使用网络共享时，为了保护用户信息的安全，需要对本地账户的网络登录进行身份验证，可以通过设置“本地安全设置”窗口中的“网络访问：本地账户的共享和安全模型”安全策略来实现，具体操作步骤如下。

Step 01 打开“本地安全策略”窗口，在左侧窗格中依次展开“安全设置”→“本地策略”→“安全选项”选项，然后在右侧窗格中找到“网络访问：本地账户的共享和安全模型”选项，如下图所示。



Step 02 双击该选项，打开“网络访问：本地账户的共享和安全模型 属性”对话框，在该对话框的下拉列表框中选择合适的选项，如下图所示，然后依次单击“应用”和“确定”按钮，即可应用设置。



> **提示**：“网络访问：本地账户的共享和安全模型”安全策略选项用于确定如何对使用本地账户的网络登录进行身份验证，有两种模式可供选择——经典：对本地用户进行身份验证，不改变其本来身份；仅来宾：对本地用户进行身份验证，其身份为来宾。

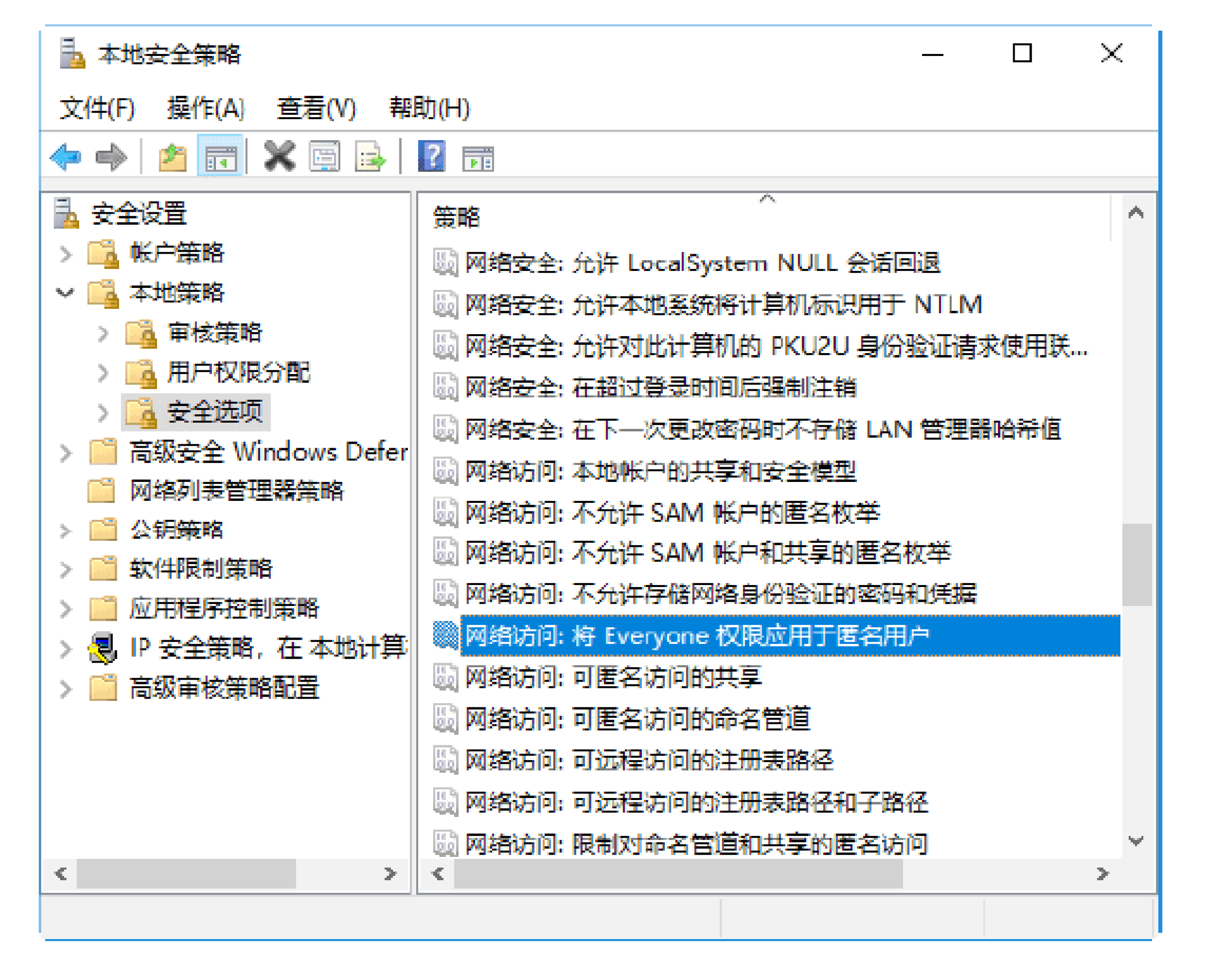
实战9：将Everyone权限应用于匿名用户



“网络访问：将Everyone权限应用于匿名用户”安全策略选项用于确定将那些附加权限授予连接到计算机的匿名连接。系统默认情况下，Everyone安全标识符（SID）会从为匿名连接创建的令牌中删除。因此，授予Everyone组的权限不会应用于匿名用户。如果启用此策略，会将Everyone SID添加到为匿名连接创建的令牌，这样匿名用户就可以访问Everyone组拥有权限的所有资源。

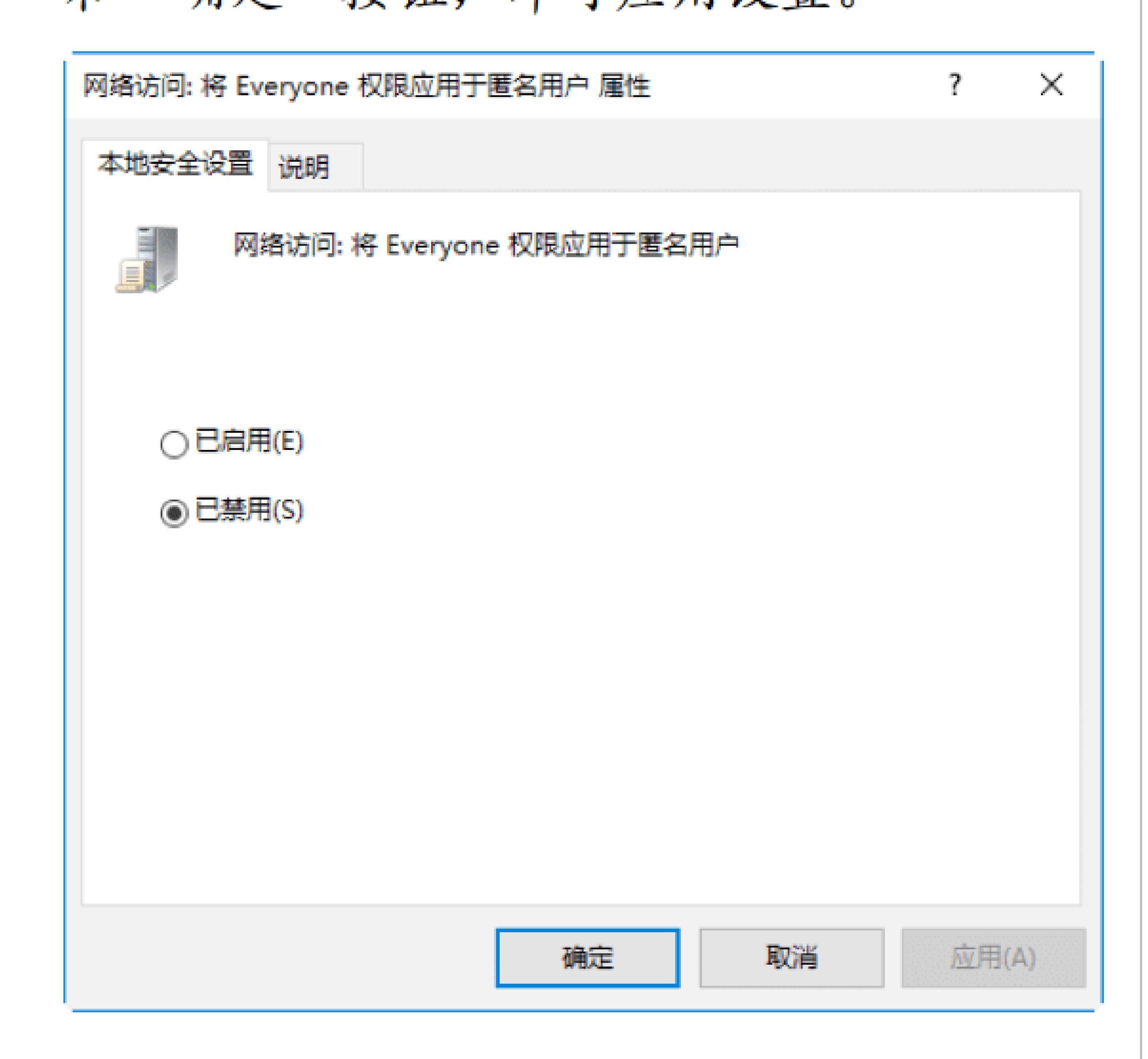
为防止出现上述情况，可以将此安全策略禁用。具体操作步骤如下。

Step 01 打开“本地安全策略”窗口，在左侧窗格中依次展开“安全设置”→“本地策略”→“安全选项”选项，然后在右侧窗格中找到“网络访问：将Everyone权限应用于匿名用户”选项，如下图所示。



Step 02 双击该选项，打开“网络访问：将Everyone权限应用于匿名用户 属性”对话

框，在该对话框中选中“已禁用”单选按钮，如下图所示，然后依次单击“应用”和“确定”按钮，即可应用设置。



13.3 通过设置组策略提高系统安全

组策略是指基于组的策略，它以Windows中的一个MMC管理单元的形式存在，通过它可以帮助系统管理员针对整个计算机或特定用户来设置多种配置，从而提升系统的安全性。

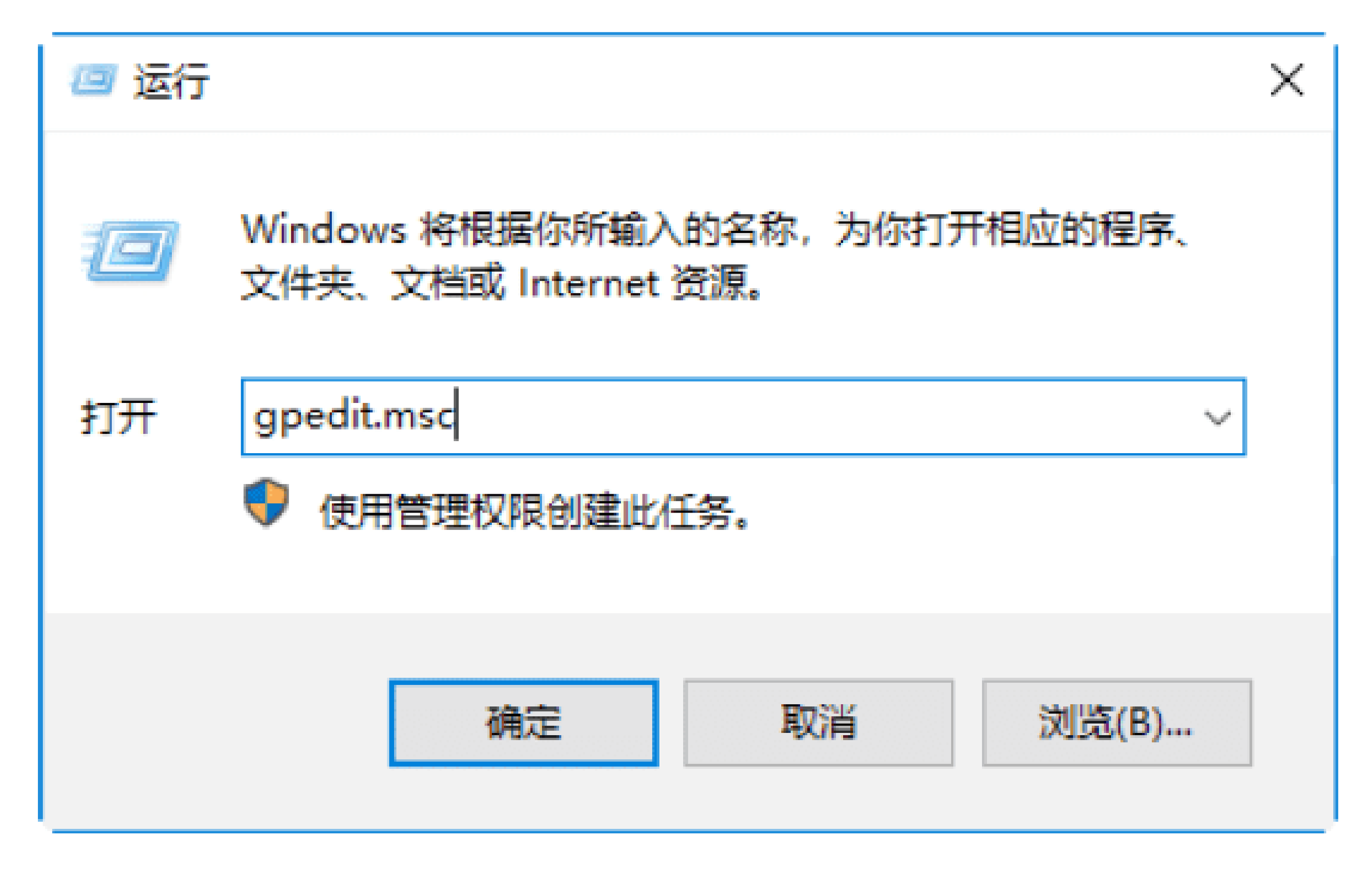


实战10：设置账户锁定策略

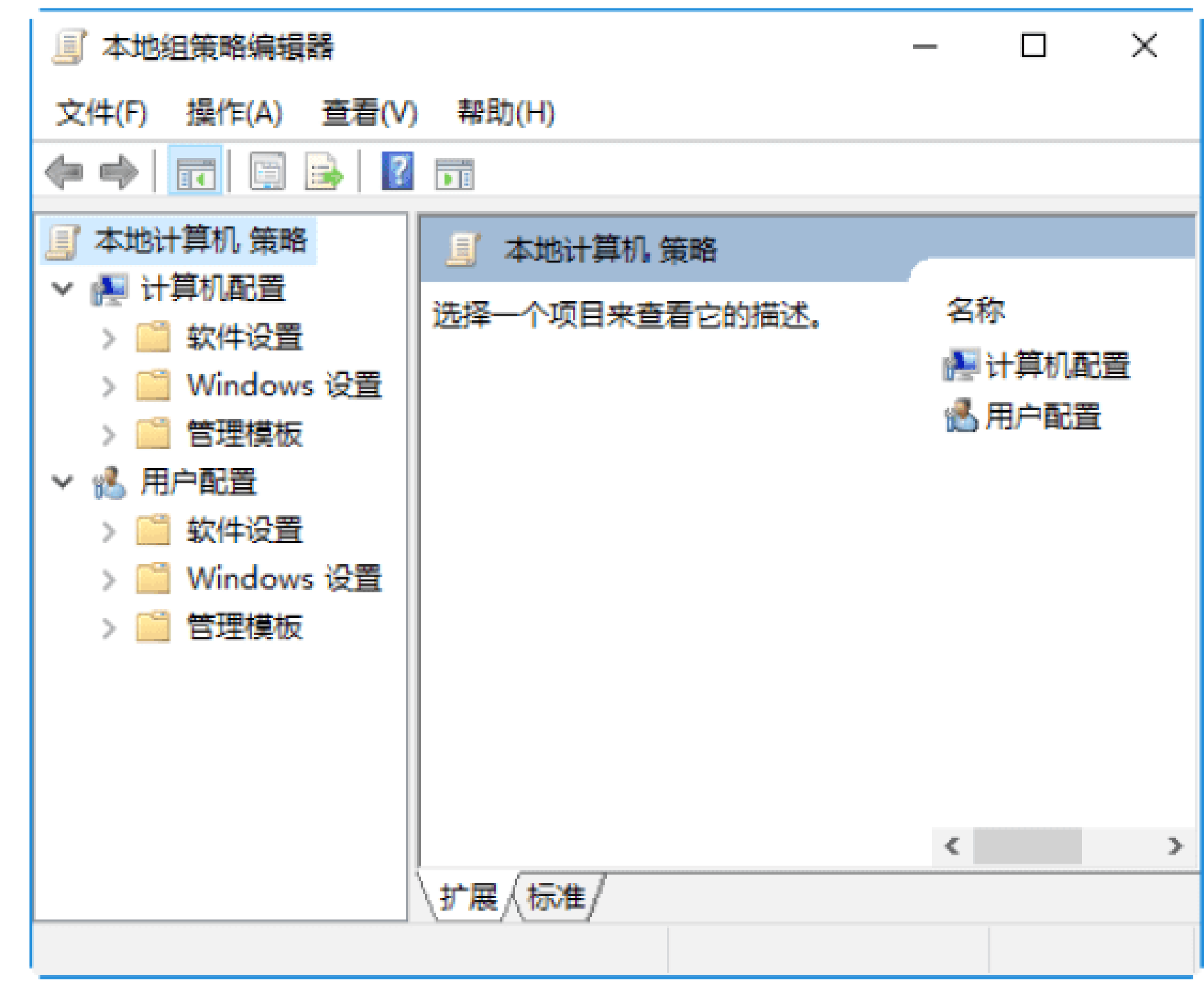
账户锁定策略是指当用户在忘记或不知道用户账户和密码的情况下，在输入*X*次（*X*代表在组策略中设置好的、可以输入的无效输入的次数）无效输入后，Windows会将登录置为锁定状态。当Windows将登录设置为锁定状态后，需要经过一定时间才能被重新启动，这样黑客便不会轻易地破解出用户账户和密码。

在“本地组策略编辑器”窗口中启用“账户锁定”策略的具体操作步骤如下。

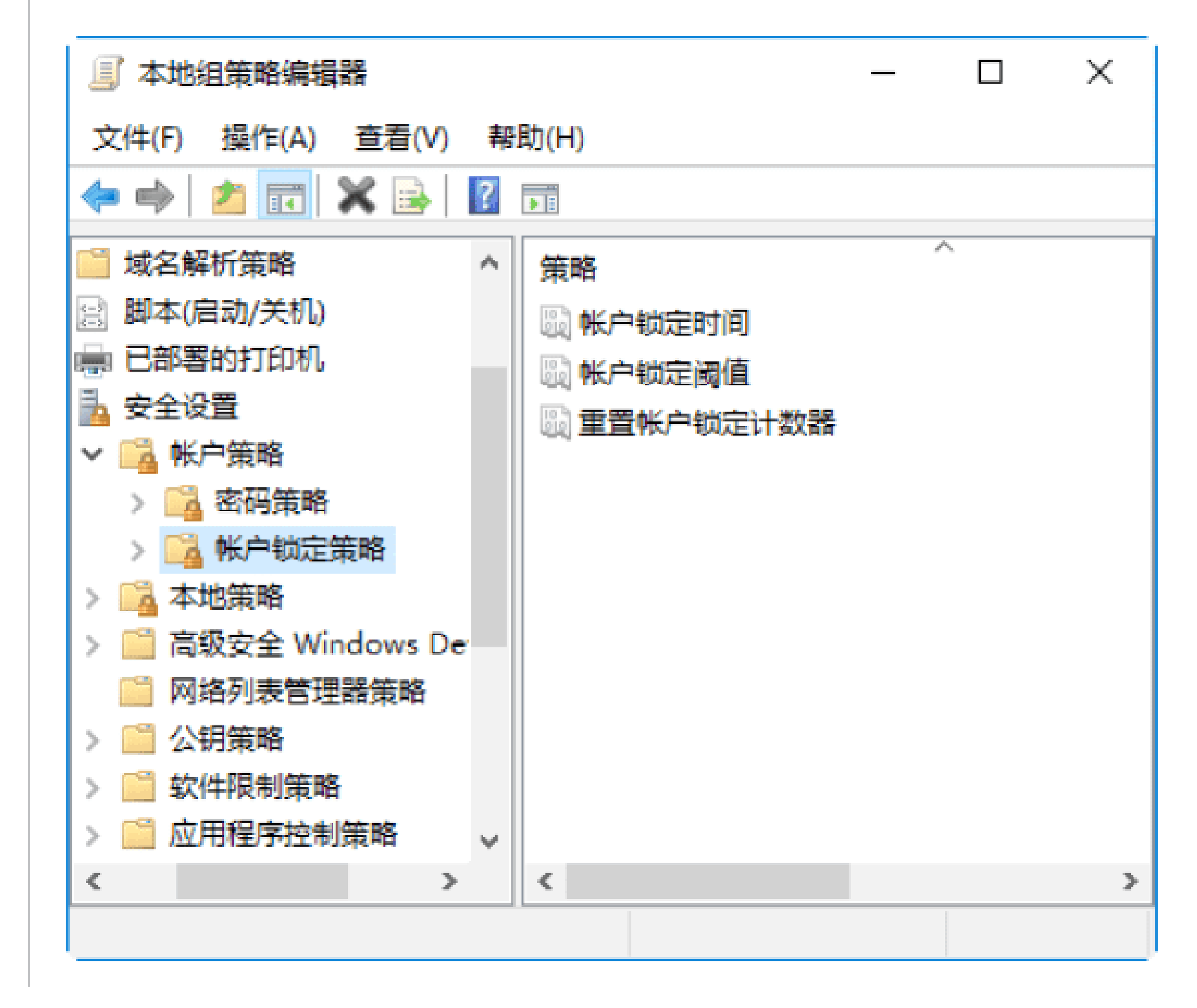
Step 01 在“运行”对话框中输入gpedit.msc命令，如下图所示。



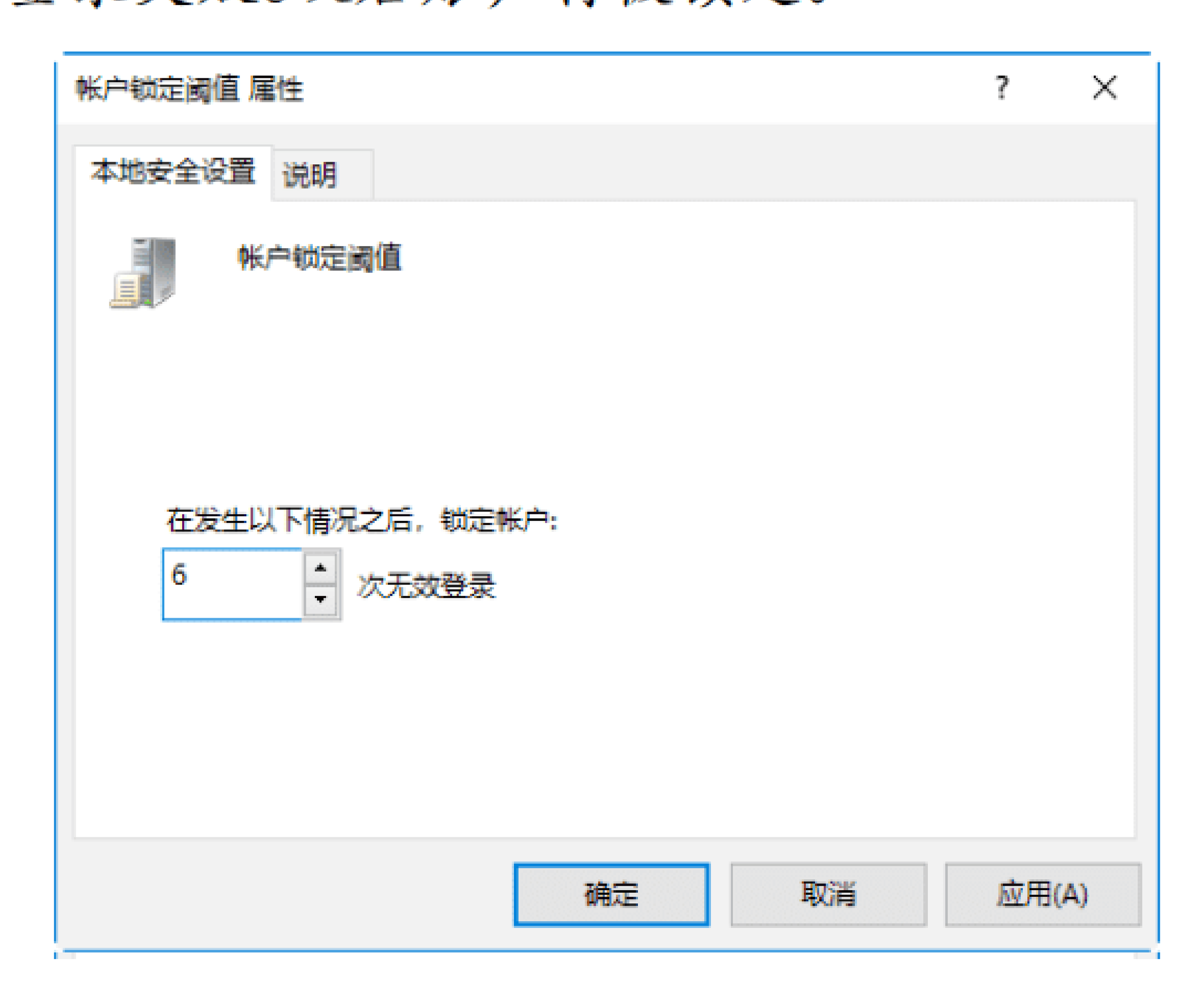
Step 02 单击“确定”按钮，打开“本地组策略编辑器”窗口，在其中显示的组策略是当前计算机，用户如果要更改某选项，只要在该窗口选中此选项即可，如下图所示。



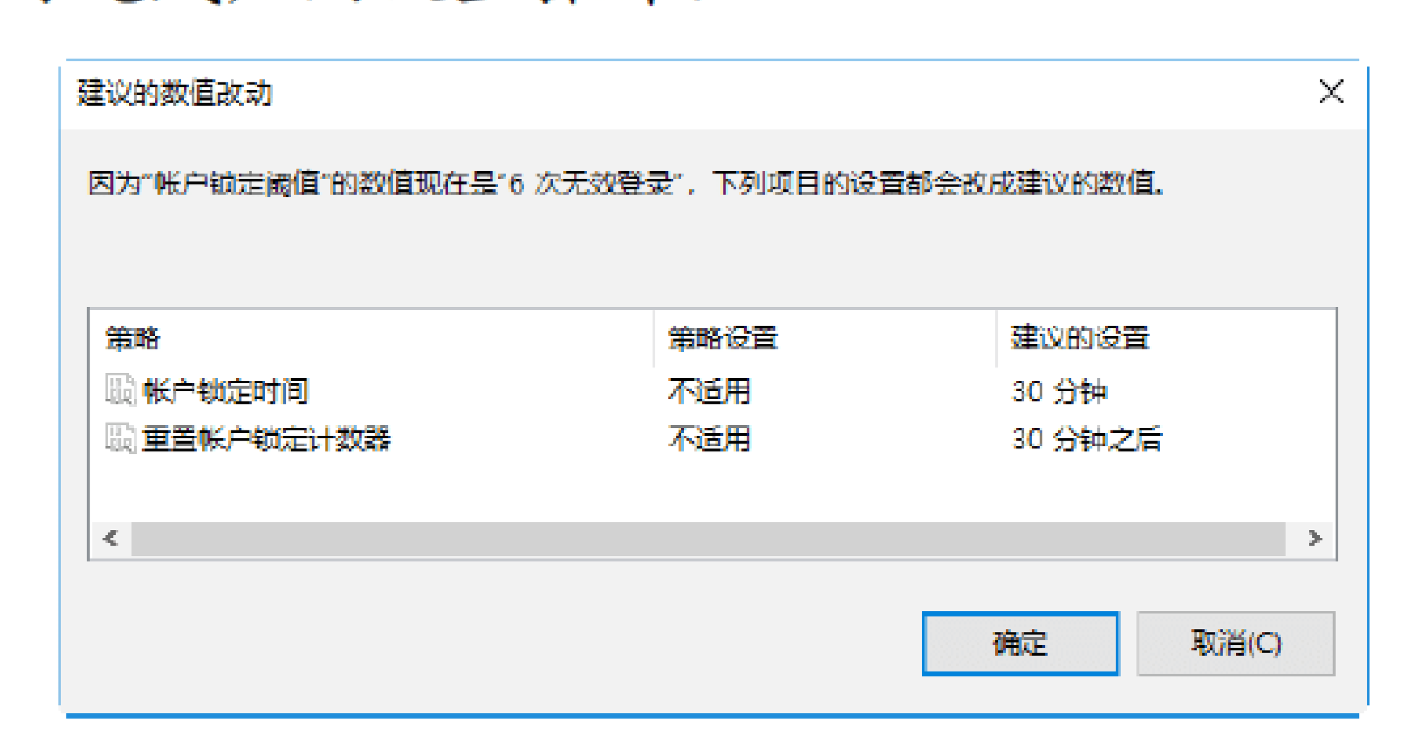
Step 03 在“本地组策略编辑器”窗口中依次展开“计算机配置”→“Windows设置”→“安全设置”→“账户策略”→“账户锁定策略”选项，进入“账户锁定策略”设置窗口，如下图所示。



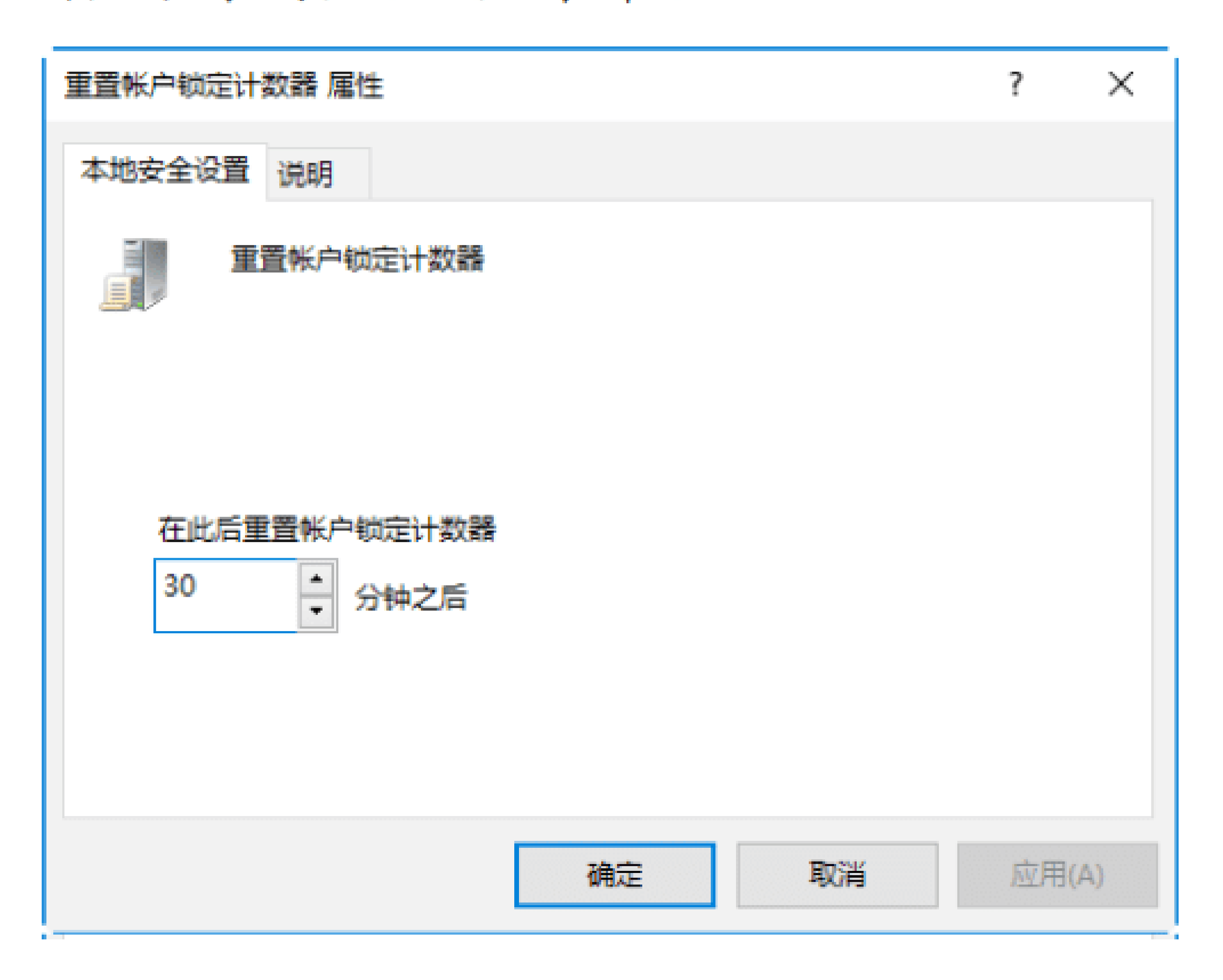
Step 04 在右侧“策略”列表中双击“账户锁定阈值”选项，打开“账户锁定阈值 属性”对话框，如下图所示。根据实际情况输入相应的数字，这里输入的是6，即表明登录失败6次后账户将被锁定。



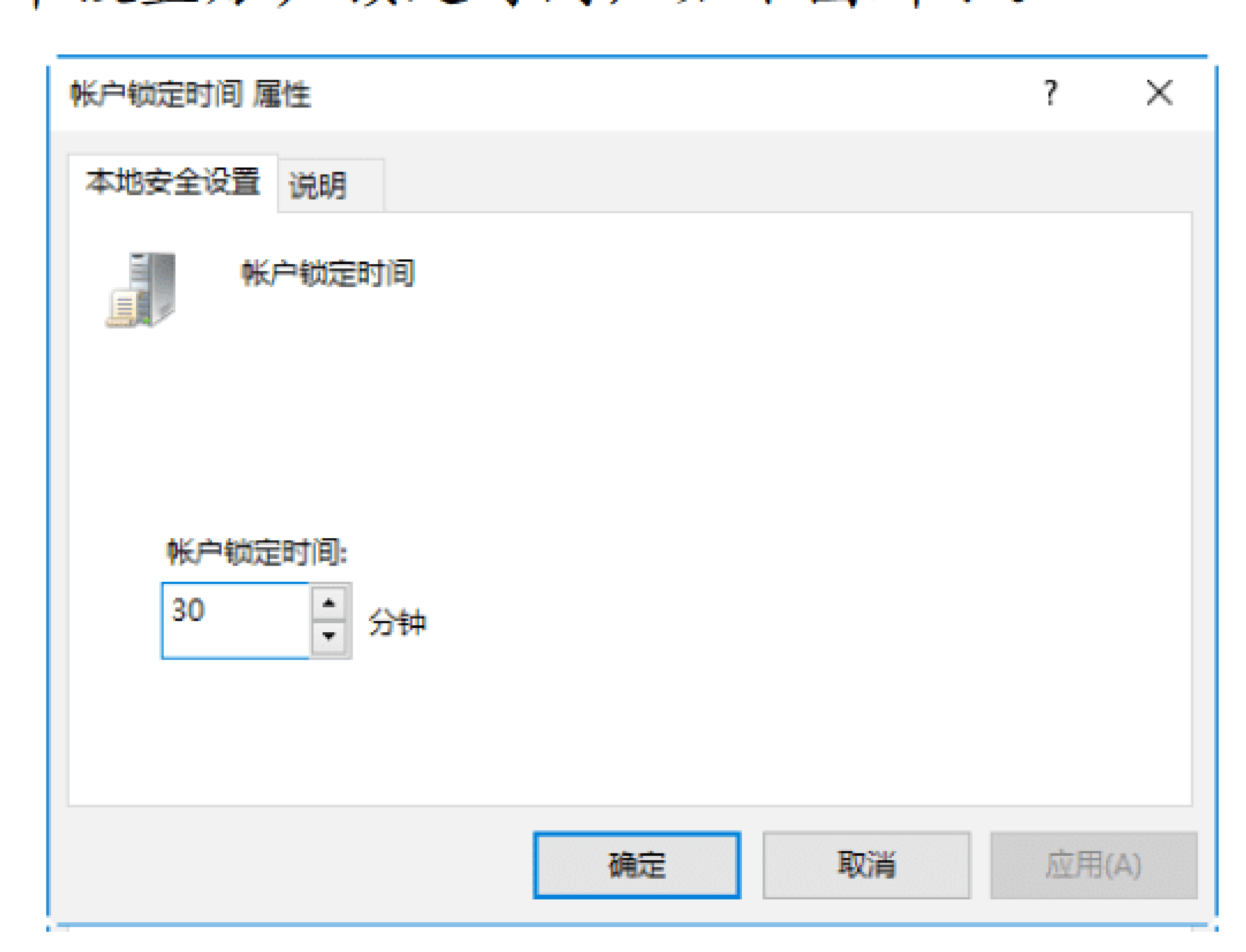
Step 05 单击“应用”按钮，打开“建议的数值改动”对话框，单击“确定”按钮，即可完成应用设置操作。



Step 06 在“账户锁定策略”设置窗口中的“策略”列表中双击“重置账户锁定计数器”选项，打开“重置账户锁定计数器 属性”对话框，在其中设置复位账户锁定计数器的时间，如下图所示。



Step 07 在“账户锁定策略”设置窗口的“策略”列表中双击“账户锁定时间”选项，打开“账户锁定时间 属性”对话框，在其中设置账户锁定时间，如下图所示。

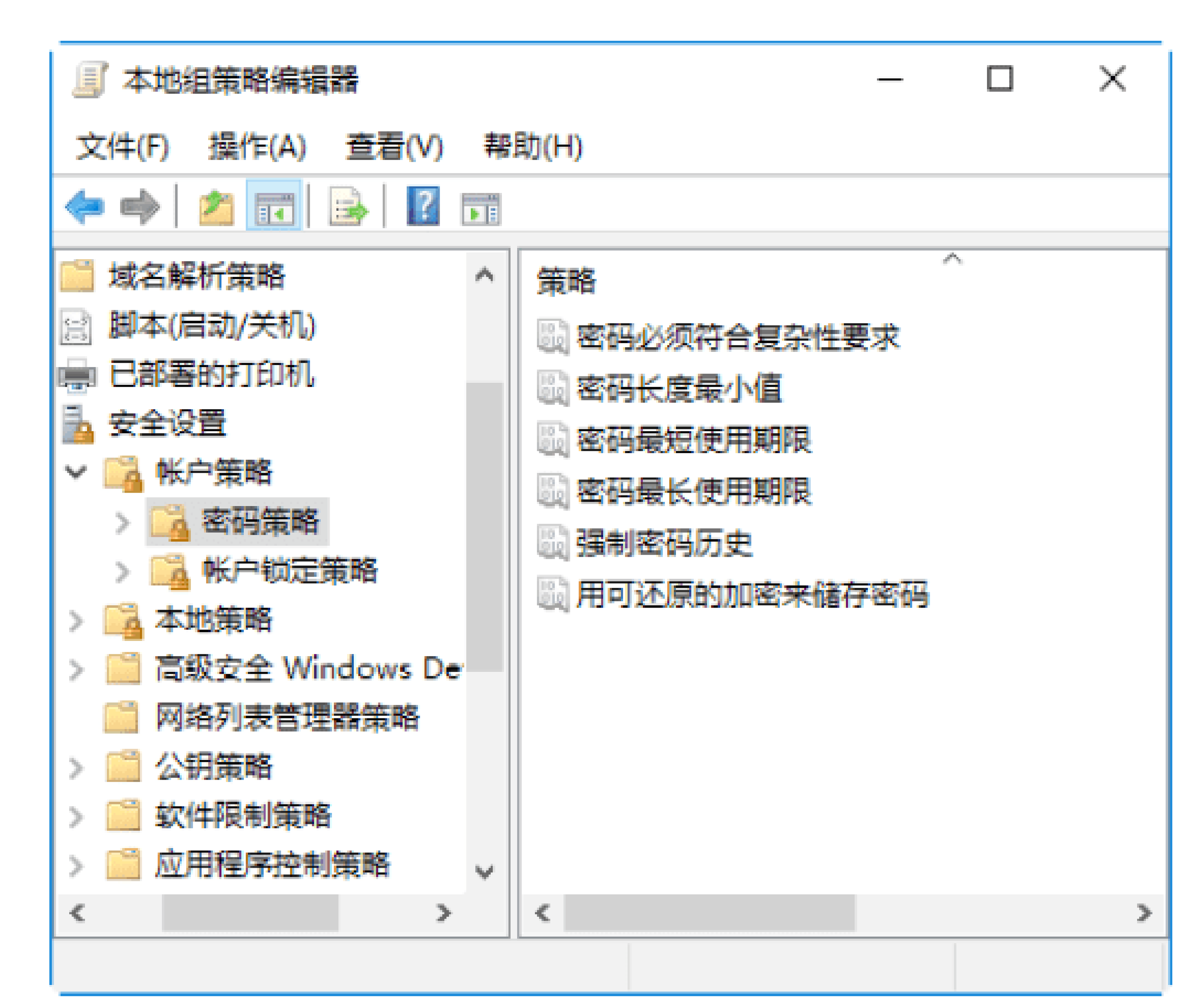


实战11：设置账户密码策略

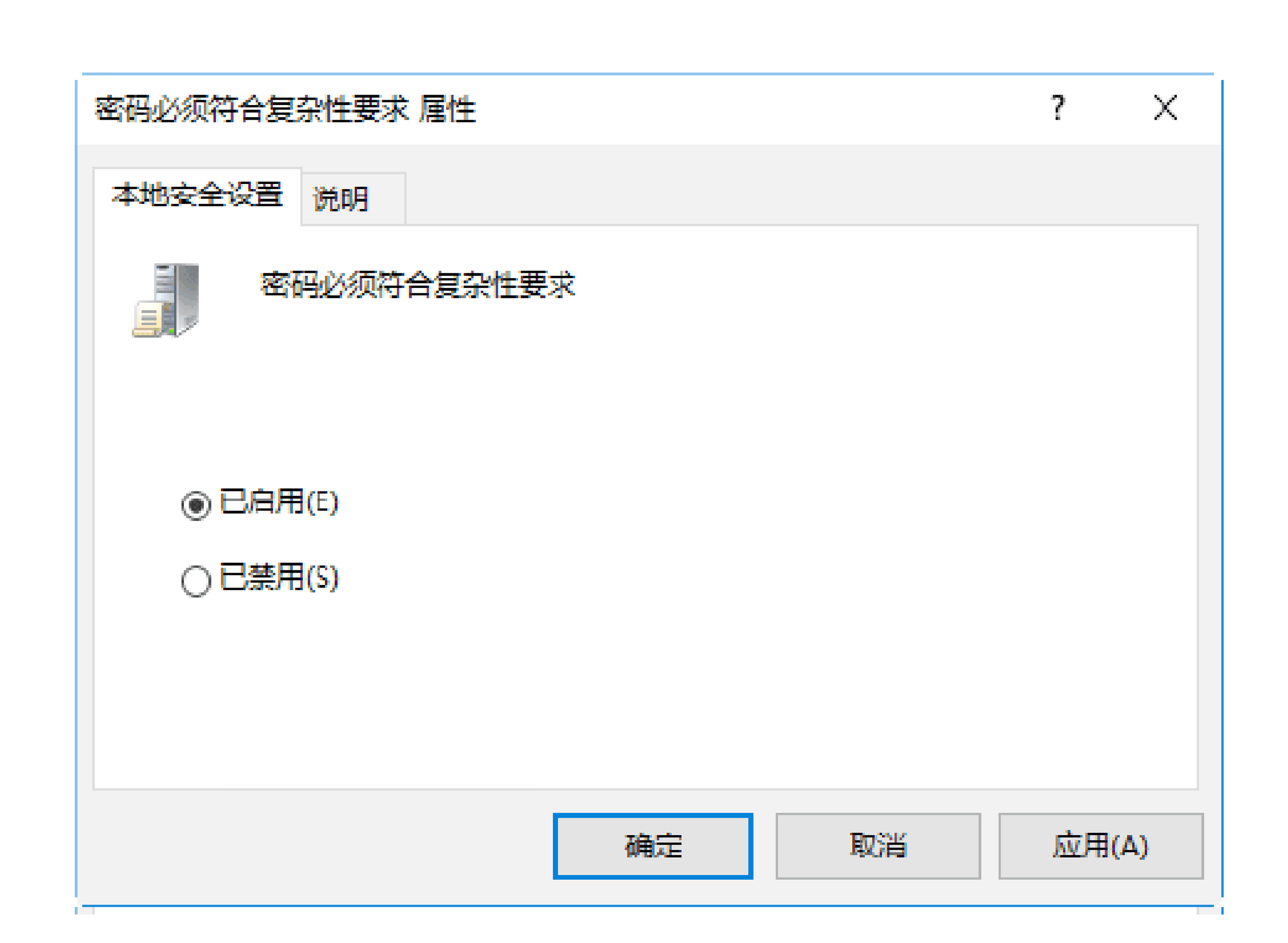


密码是用户登录操作系统的凭证，只有输入了正确的密码，用户才能正常进入系统。通过设置密码策略，可以加强系统的安全性，在一定程度上能够防止其他用户登录自己的计算机。具体操作步骤如下。

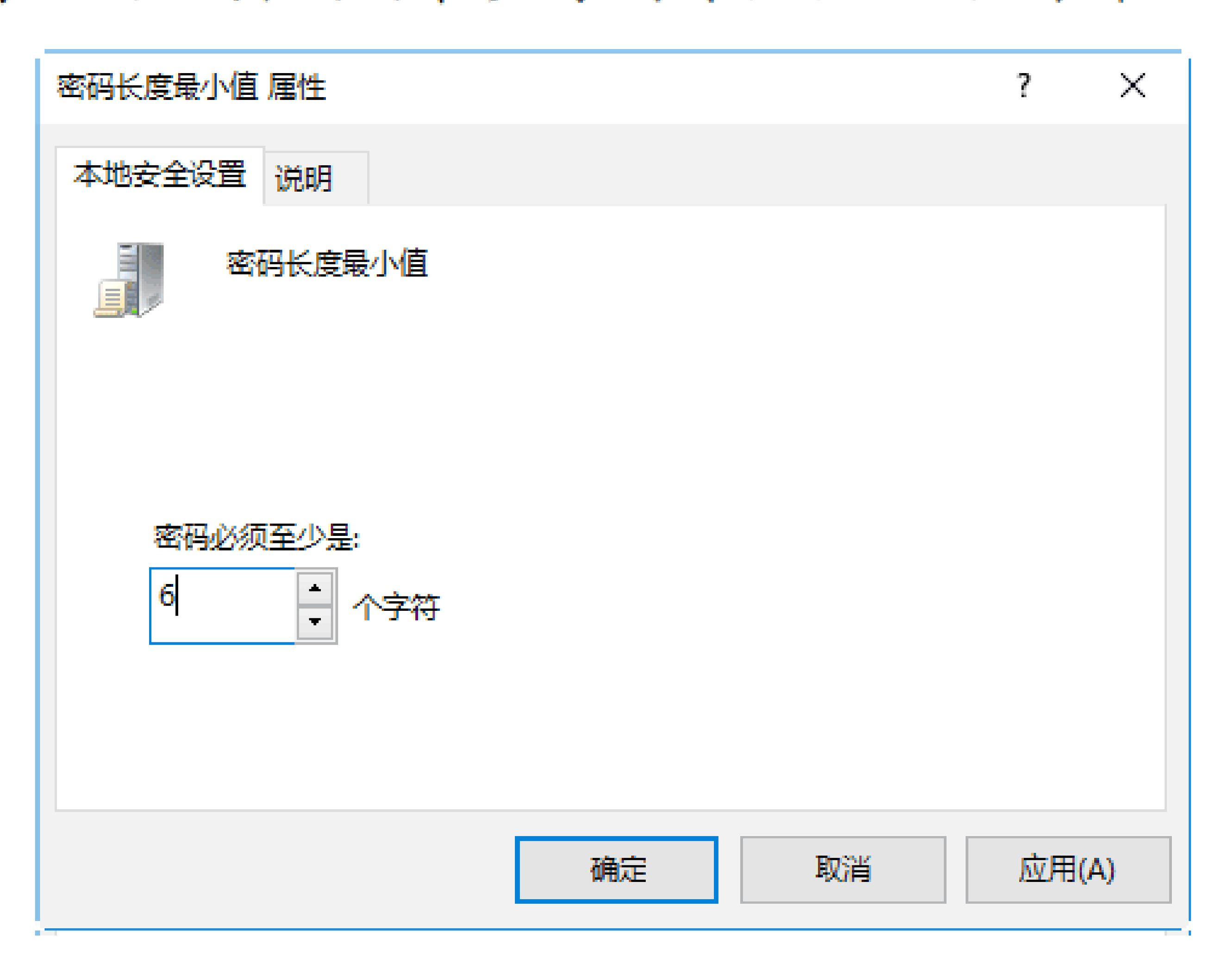
Step 01 在“本地组策略编辑器”窗口中依次展开“计算机配置”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”选项，进入“密码策略”设置界面，如下图所示。



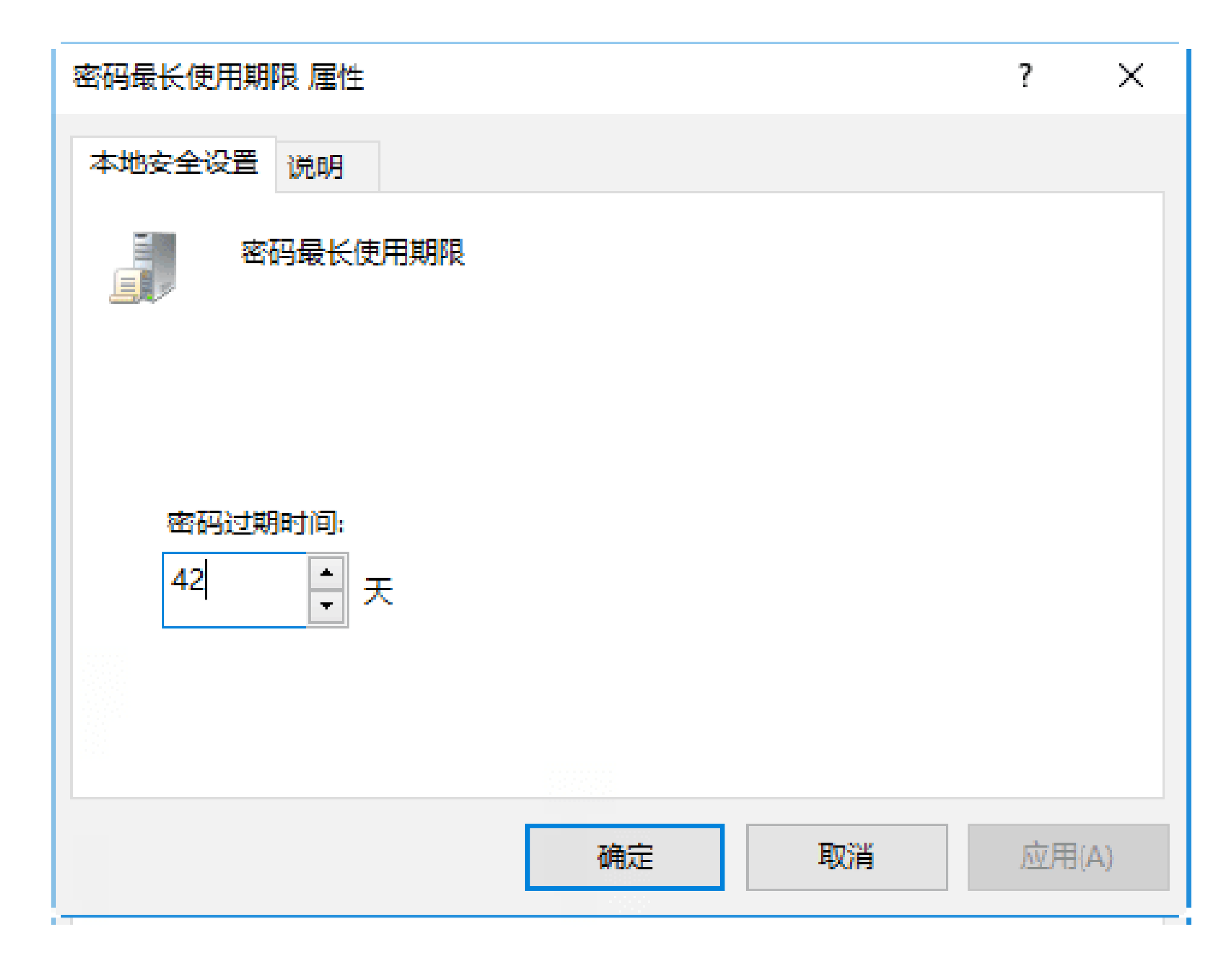
Step 02 双击“密码必须符合复杂性要求”选项，打开“密码必须符合复杂性要求 属性”对话框，选中“已启用”单选按钮，即可启用密码复杂性要求，如下图所示。



Step 03 双击“密码长度最小值”选项，打开“密码长度最小值 属性”对话框，根据实际情况输入密码的最少字符个数，如下图所示。



Step 04 双击“密码最长使用期限”选项，打开“密码最长使用期限 属性”对话框，在“密码过期时间”文本框中设置密码过期的天数，如下图所示。

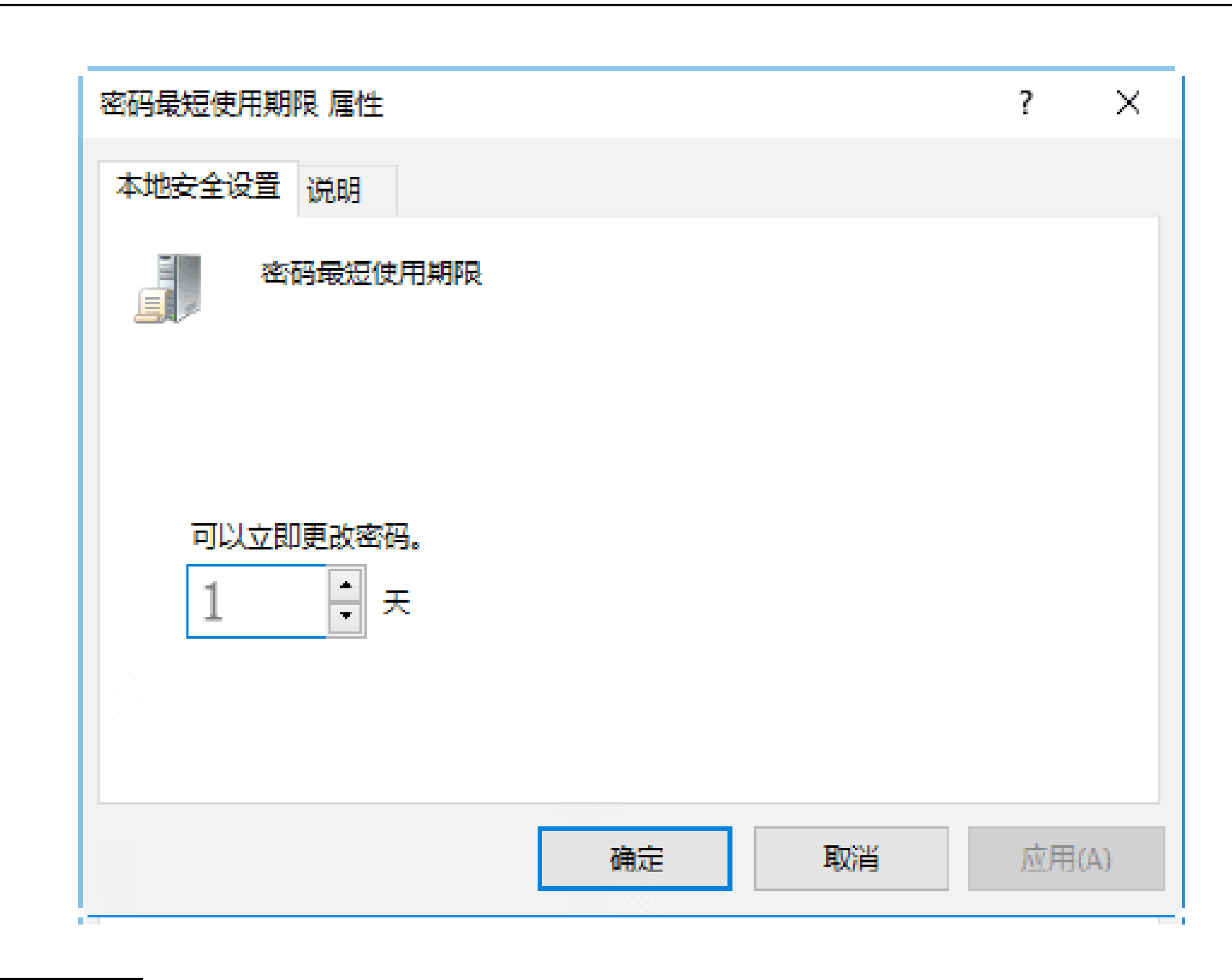




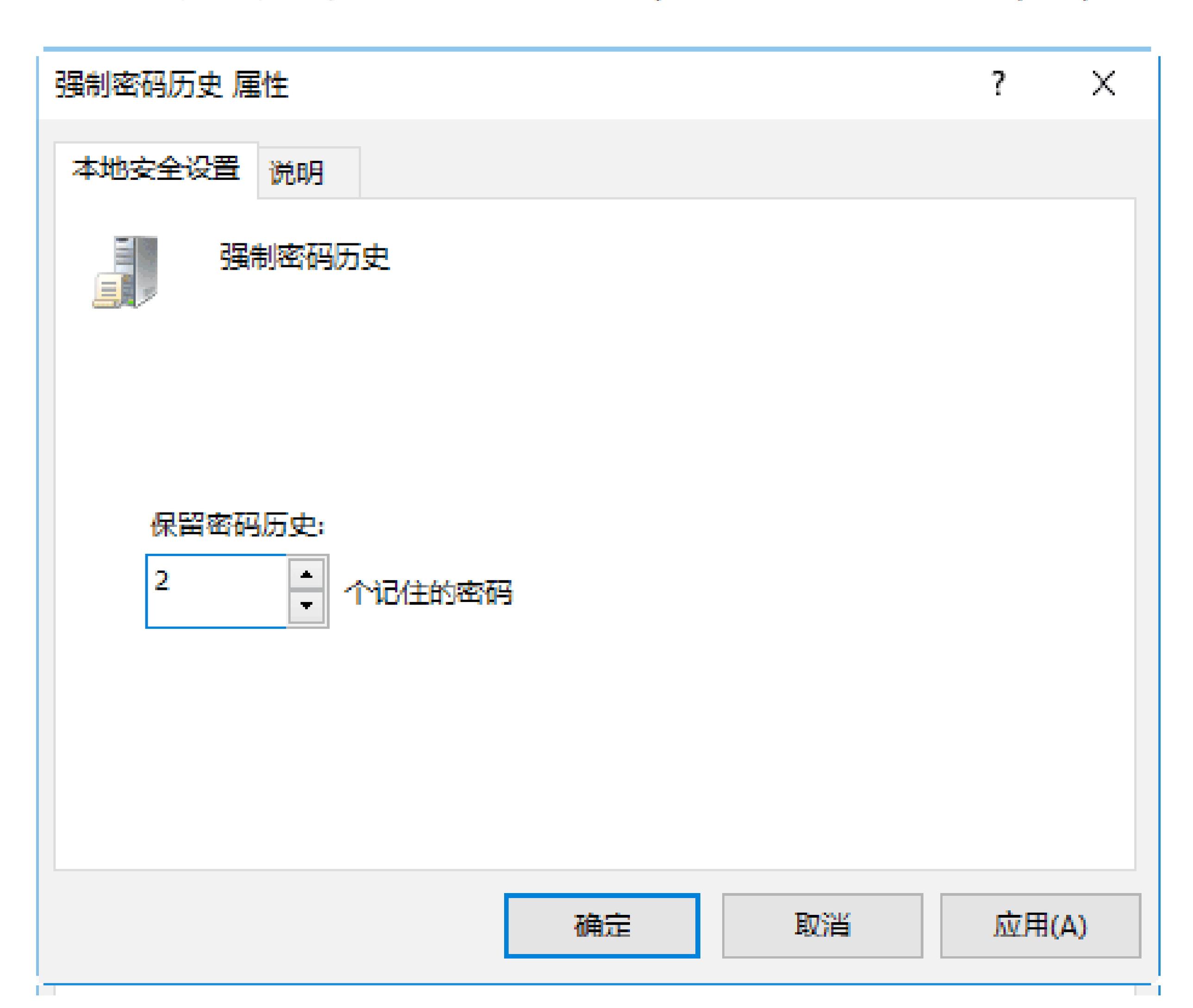
提示：由于空密码和太短的密码都很容易被专用破解软件猜测到，为减小密码破解的可能性，密码应该尽量长。有特权用户（如Administrators组的用户）的密码长度最好超过12个字符。一个用来加强密码长度的方法是使用不在默认字符集中的字符。

Step 05 双击“密码最短使用期限”选项，打开“密码最短使用期限 属性”对话框，根据实际情况设置密码最短使用期限后，单击“确定”按钮即可，如下图所示。

注意：默认情况下，用户可在任何时间修改自己的密码，因此，用户可以更换一个密码，立刻再更改回原来的旧密码。这个选项可用的设置范围是0（密码可随时修改）或1～998（天），建议设置为1天，如下图所示。



Step 06 双击“强制密码历史”选项，打开“强制密码历史 属性”对话框，根据个人情况设置保留密码历史的个数，如下图所示。

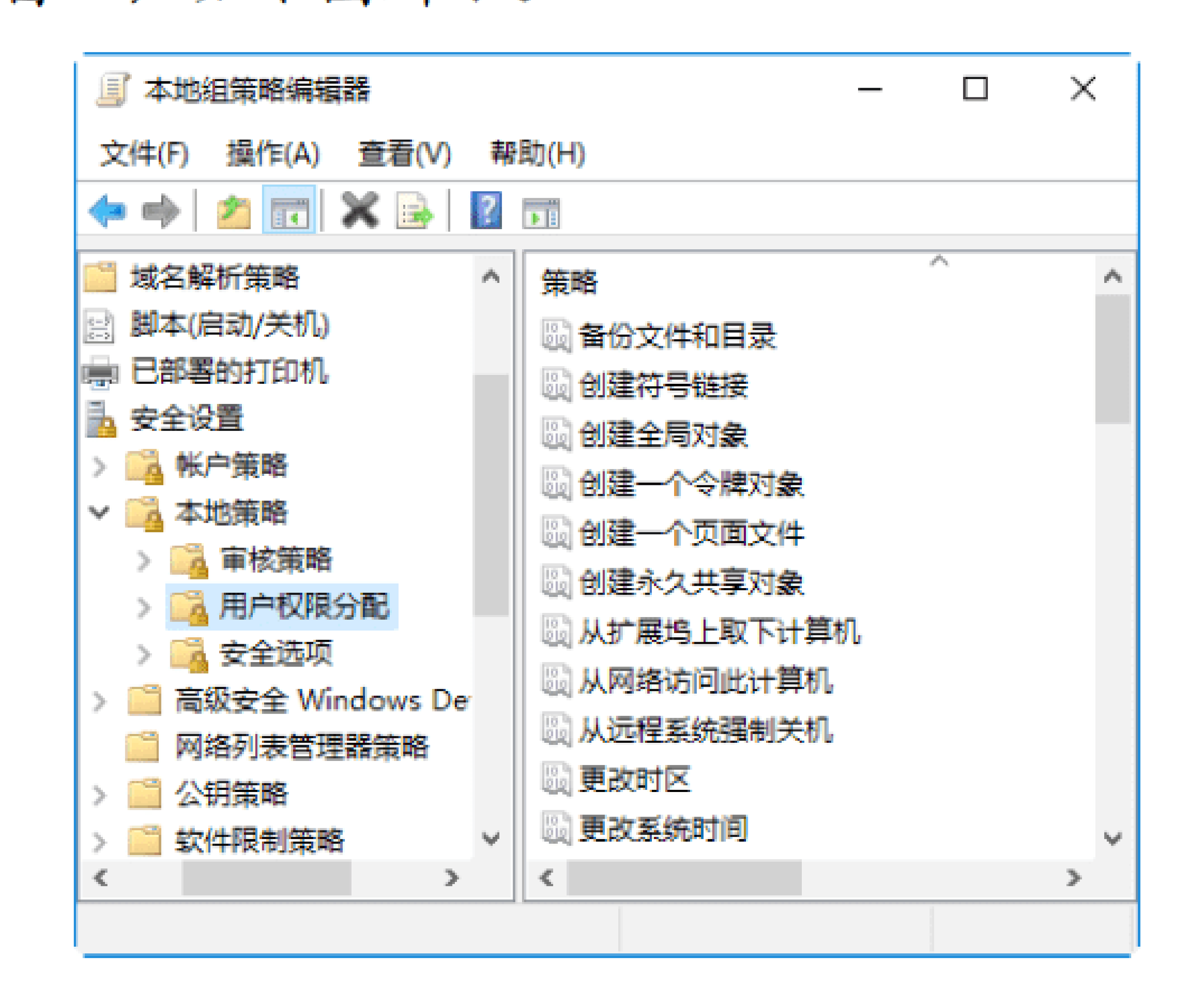


实战12：设置用户权限分配

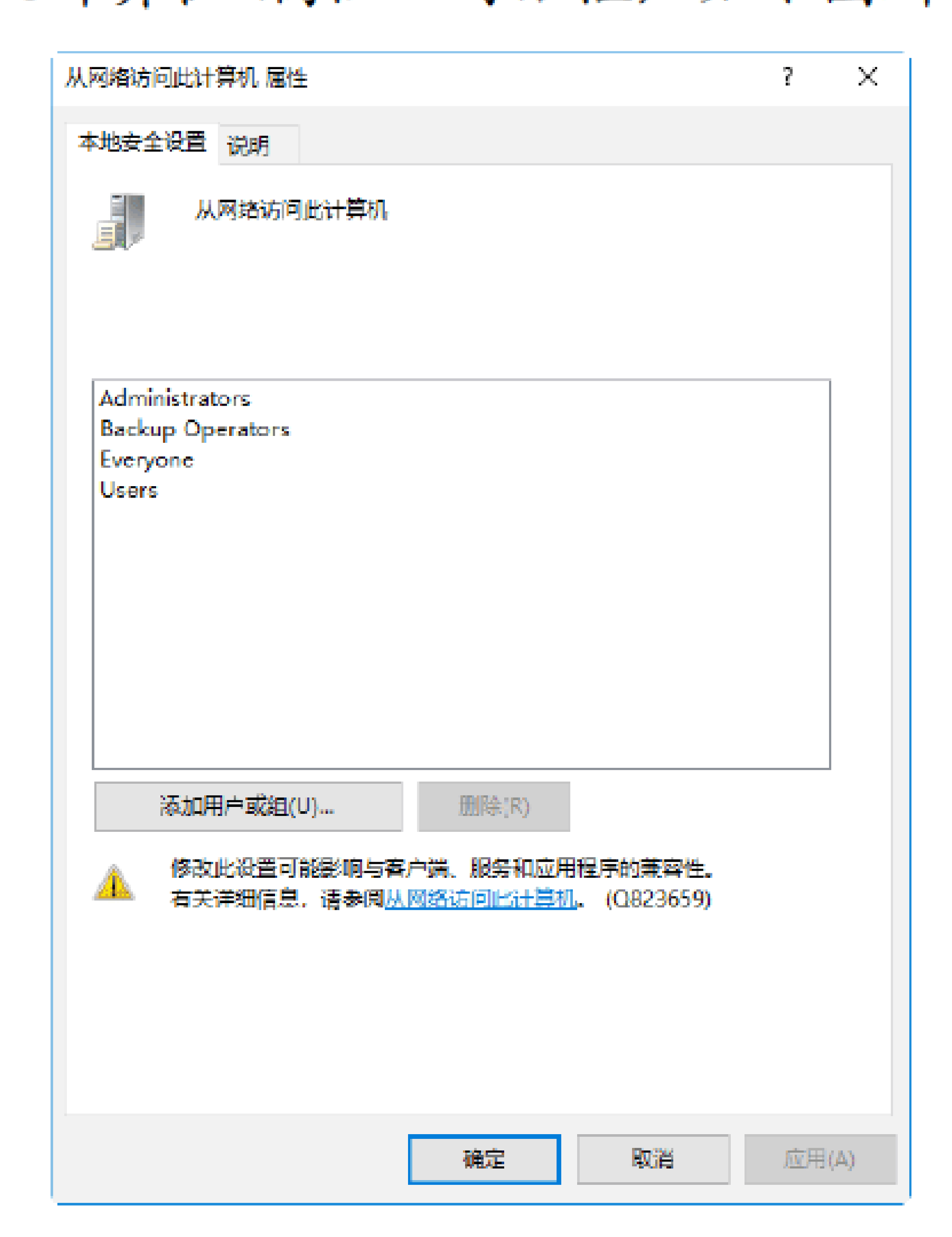
当多人共用一台计算机时，可以在“本地组策略编辑器”窗口中设置不同的用户权限，限制黑客访问该计算机时要进行的某些操作。具体操作步骤如下。

Step 01 在“本地组策略编辑器”窗口中依次展开“计算机配置”→“Windows设

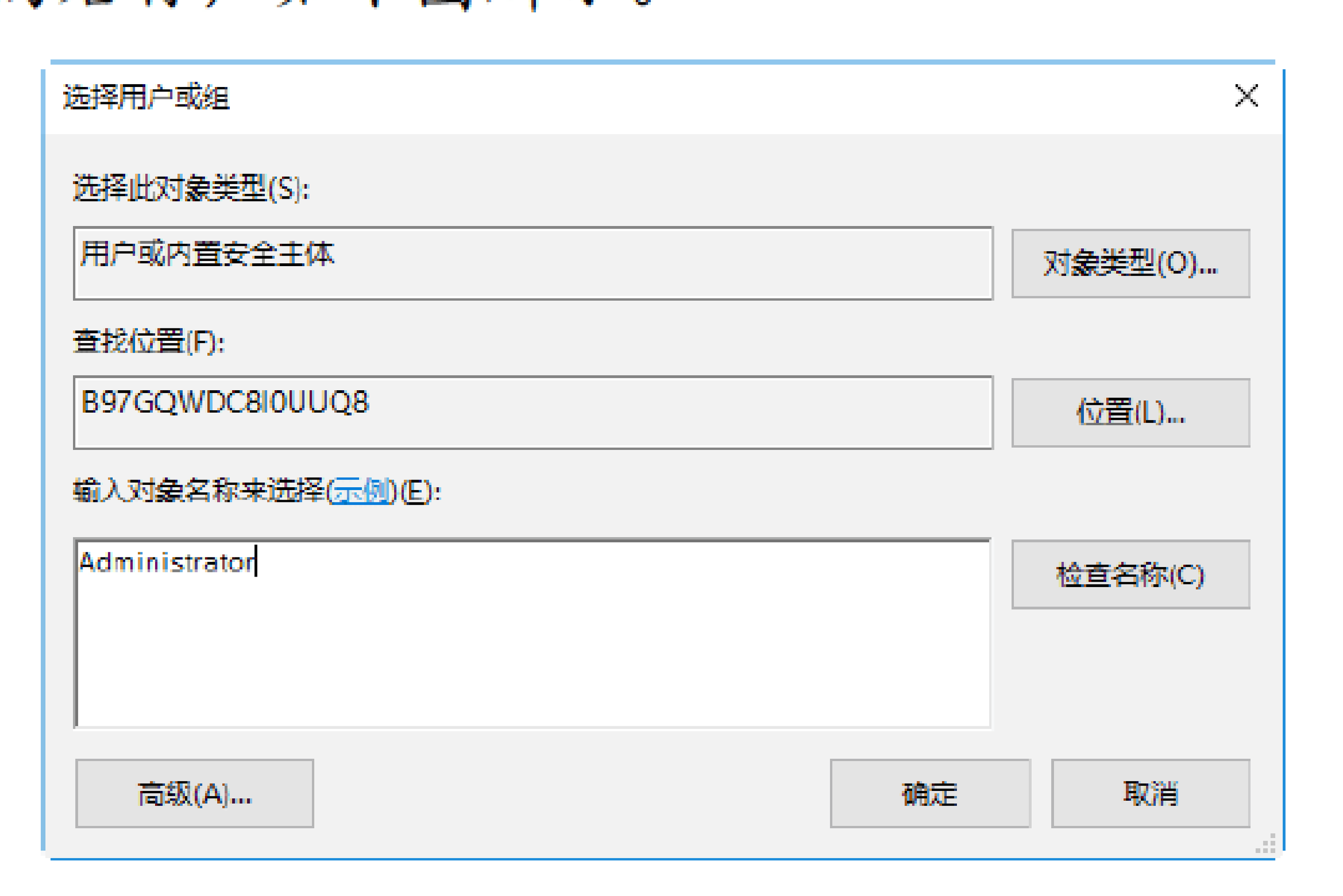
置”→“安全设置”→“本地策略”→“用户权限分配”选项，进入“用户权限分配”窗口，如下图所示。



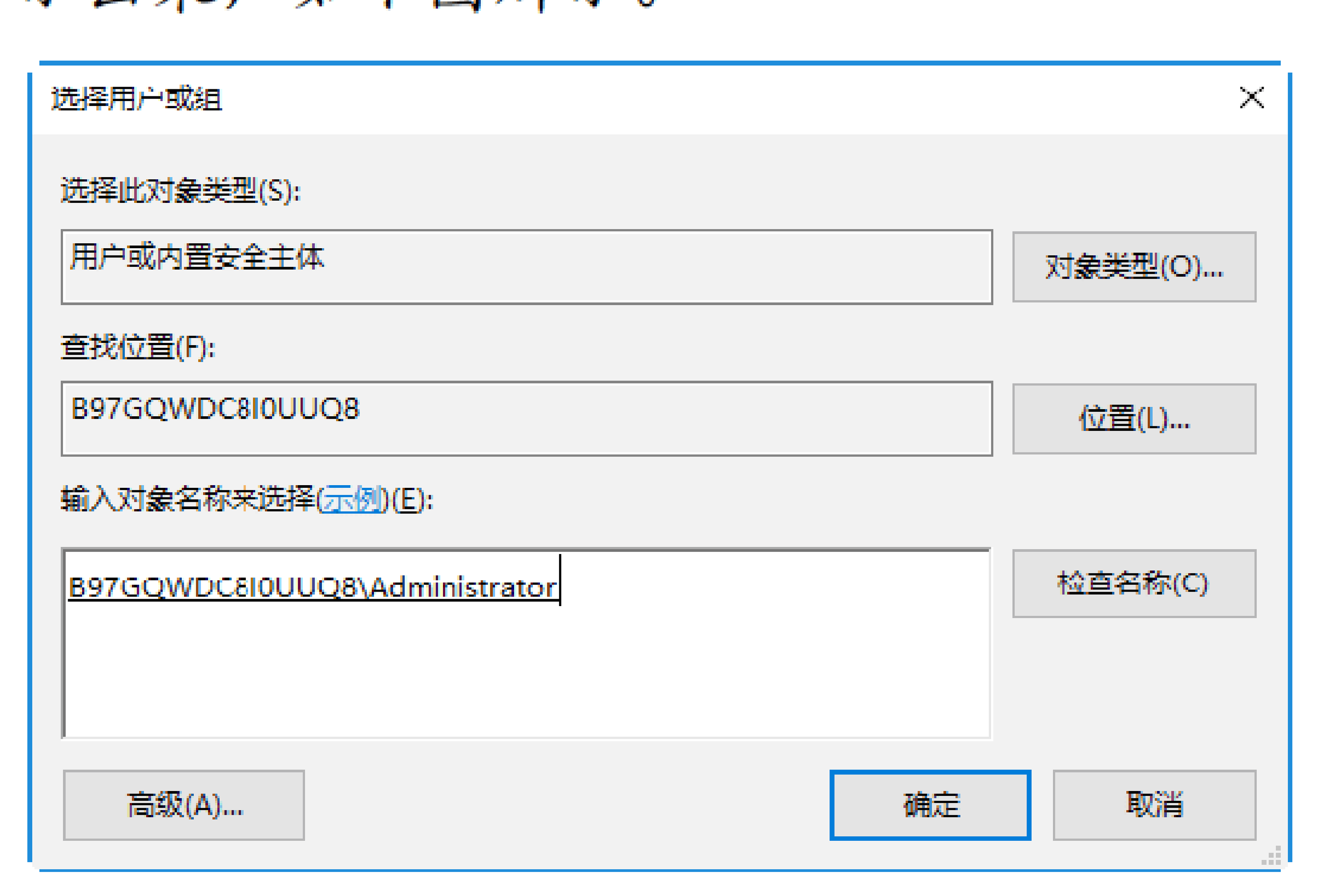
Step 02 双击需要改变的用户权限选项，如“从网络访问此计算机”选项，即可打开“从网络访问此计算机 属性”对话框，如下图所示。



Step 03 单击“添加用户或组”按钮，打开“选择用户或组”对话框，在“输入对象名称来选择（示例）”文本框中输入添加对象的名称，如下图所示。

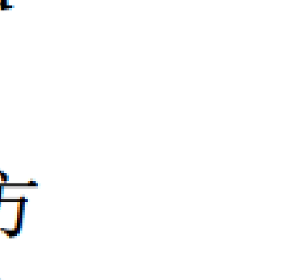


Step 04 单击“检查名称”按钮，即可对输入的名称进行检测，如果输入的名称存在，则会将检测出的名字连同这个名称一同显示出来，如下图所示。



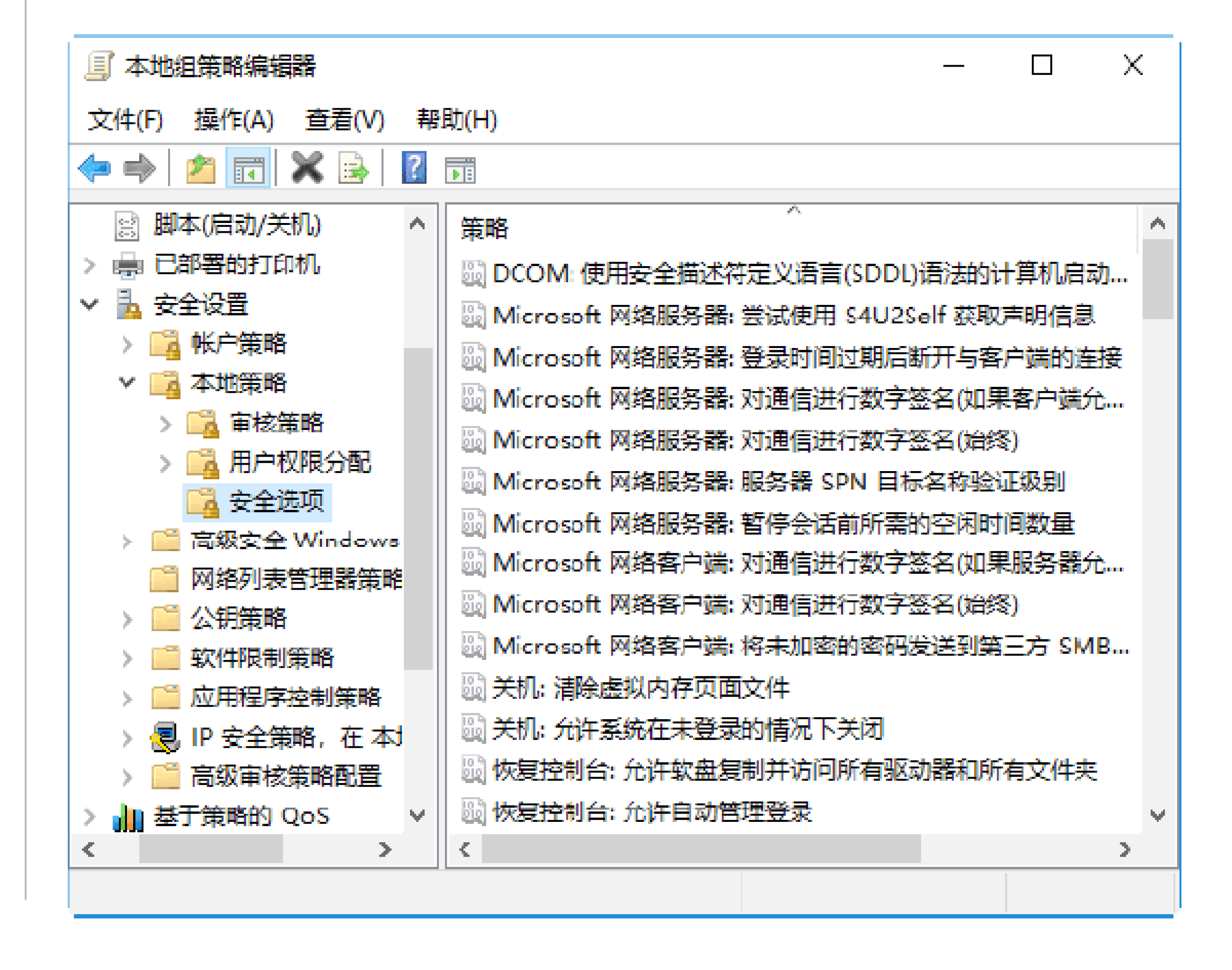
Step 05 单击“确定”按钮，即可将该对象添加到用户组中，再次单击“确定”按钮，即可完成用户权限的设置操作。

实战13：更改系统默认的账户

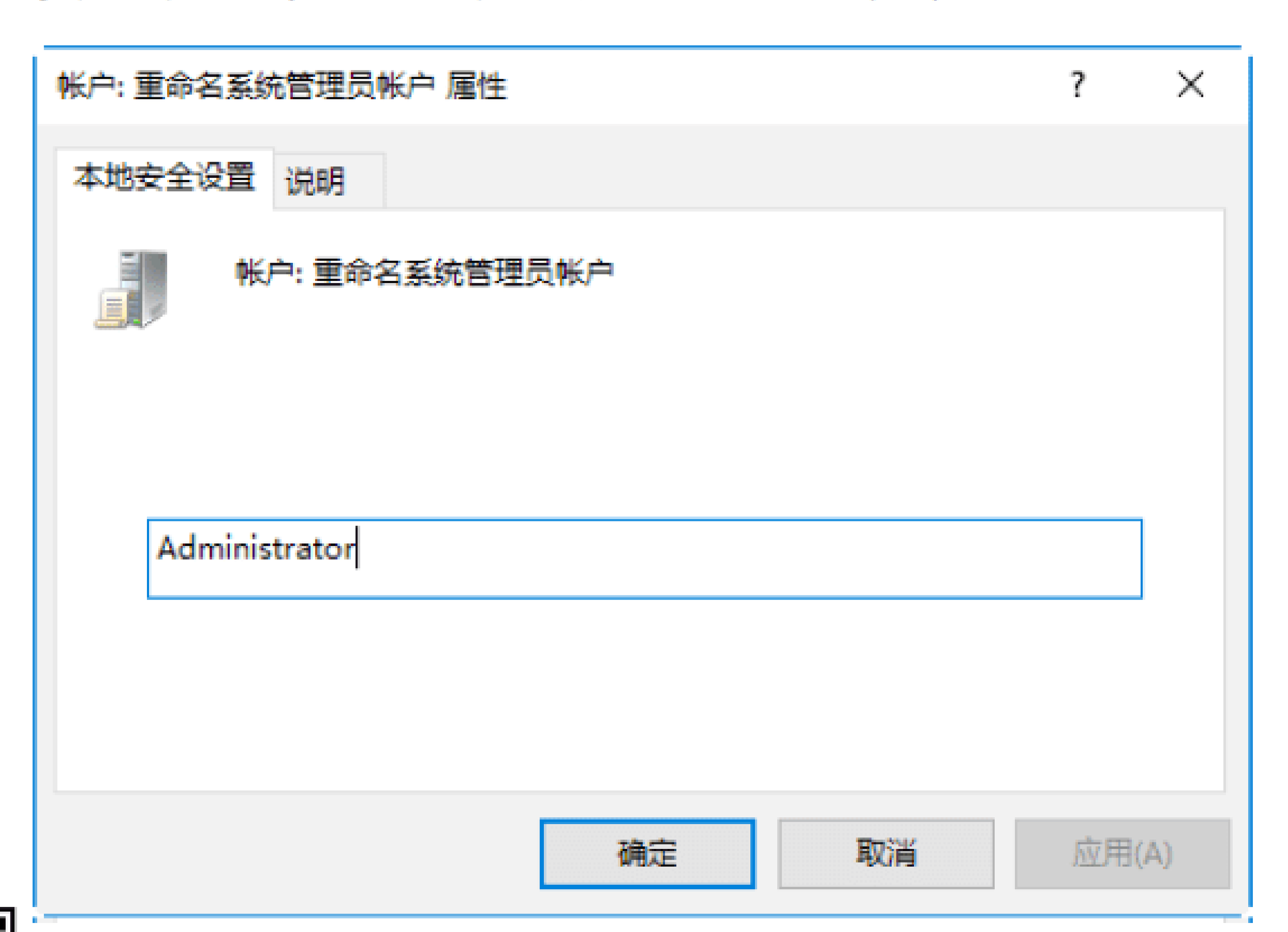


在一般情况下，在Windows中内置了Administrator和Guest两个账户，其中Administrator是具有全部权限的管理员账户。黑客往往是通过密码猜测或暴力破解方式，来获得该管理员账户信息，所以防御黑客入侵的最好办法就是改变这两个默认账户名称。具体操作步骤如下。

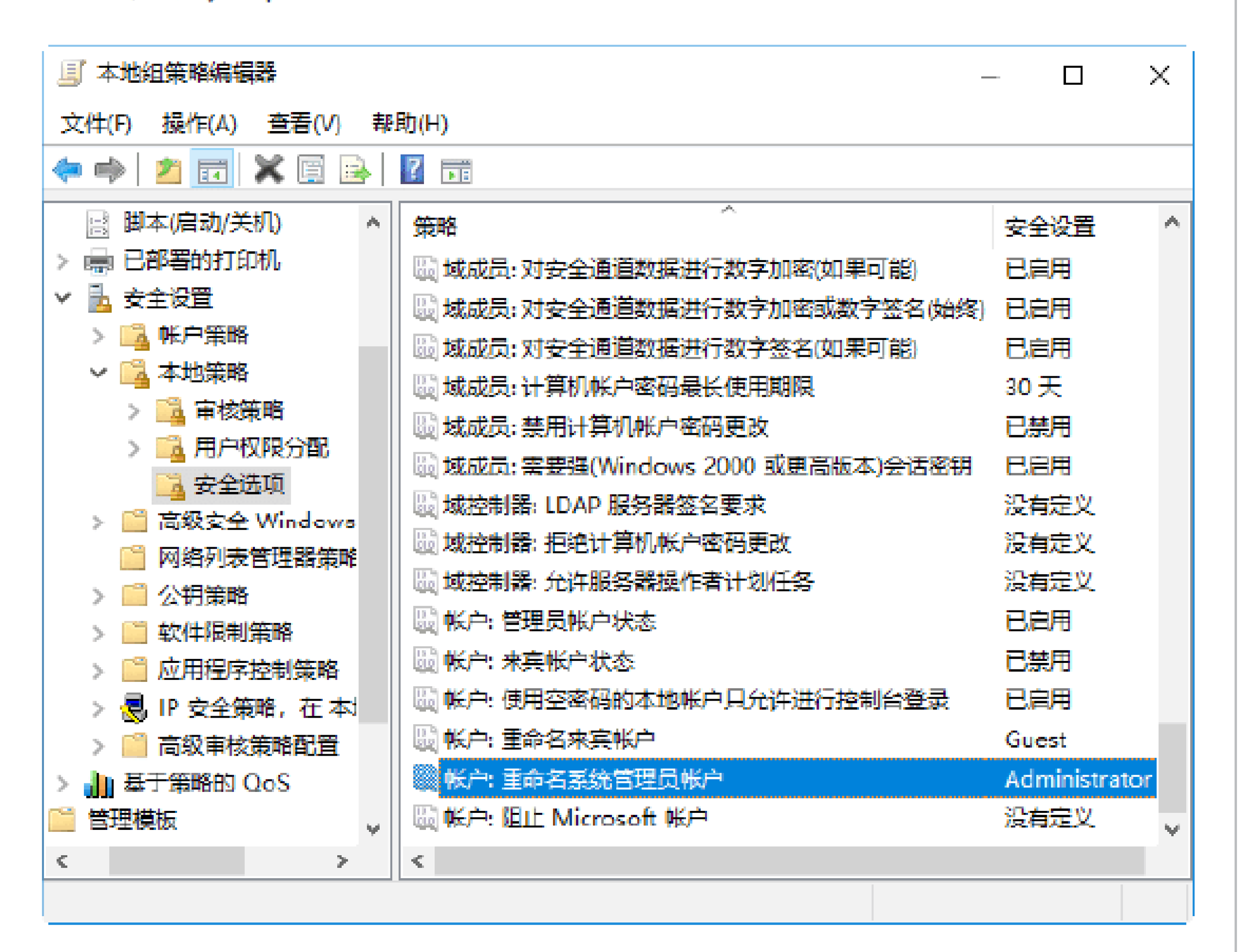
Step 01 在“本地组策略编辑器”窗口中依次展开“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“安全选项”选项，进入“安全选项”设置窗口，如下图所示。



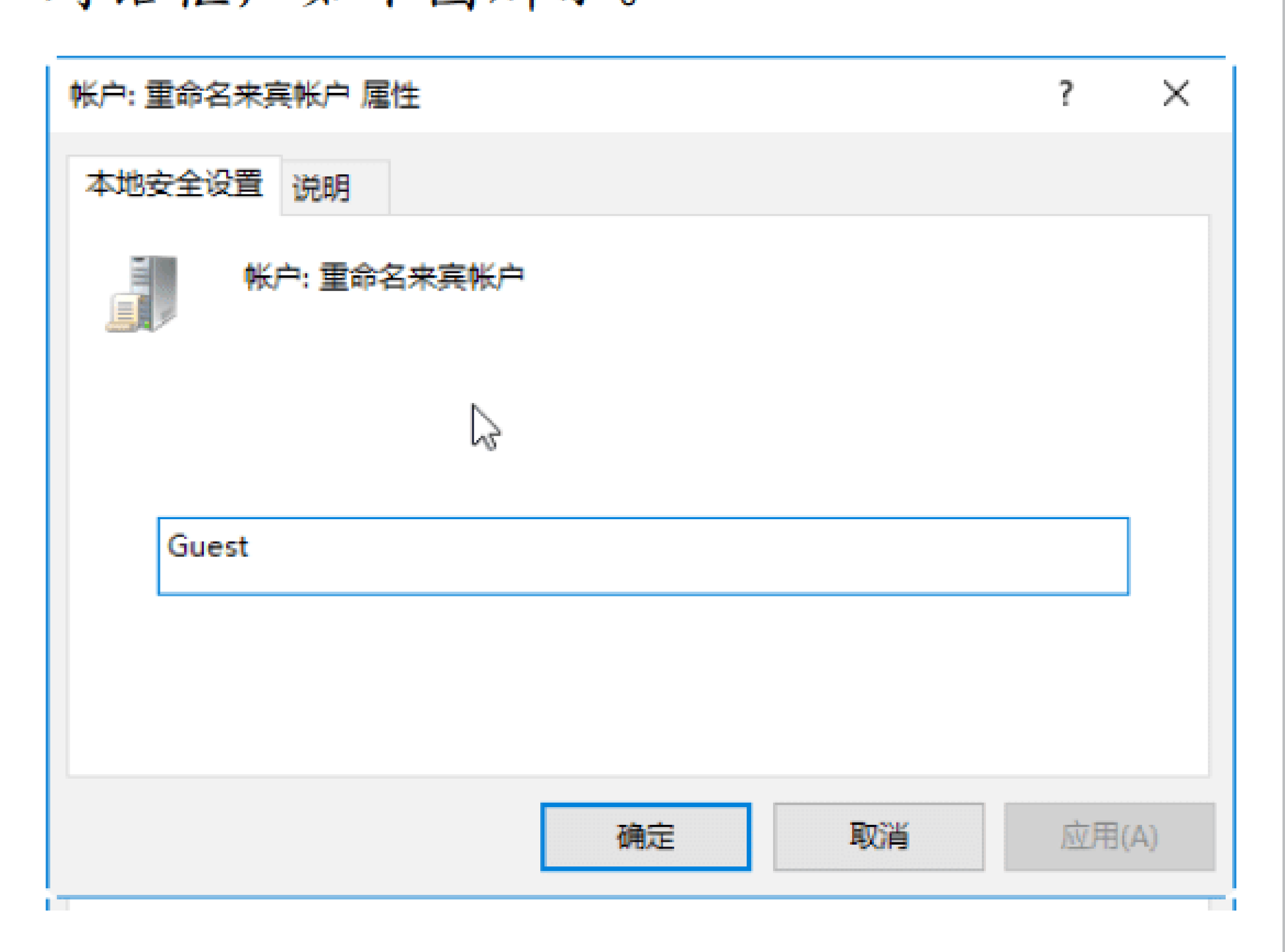
Step 02 双击“账户：重命名系统管理员账户”选项，打开“账户：重命名系统管理员账户 属性”对话框，如下图所示。



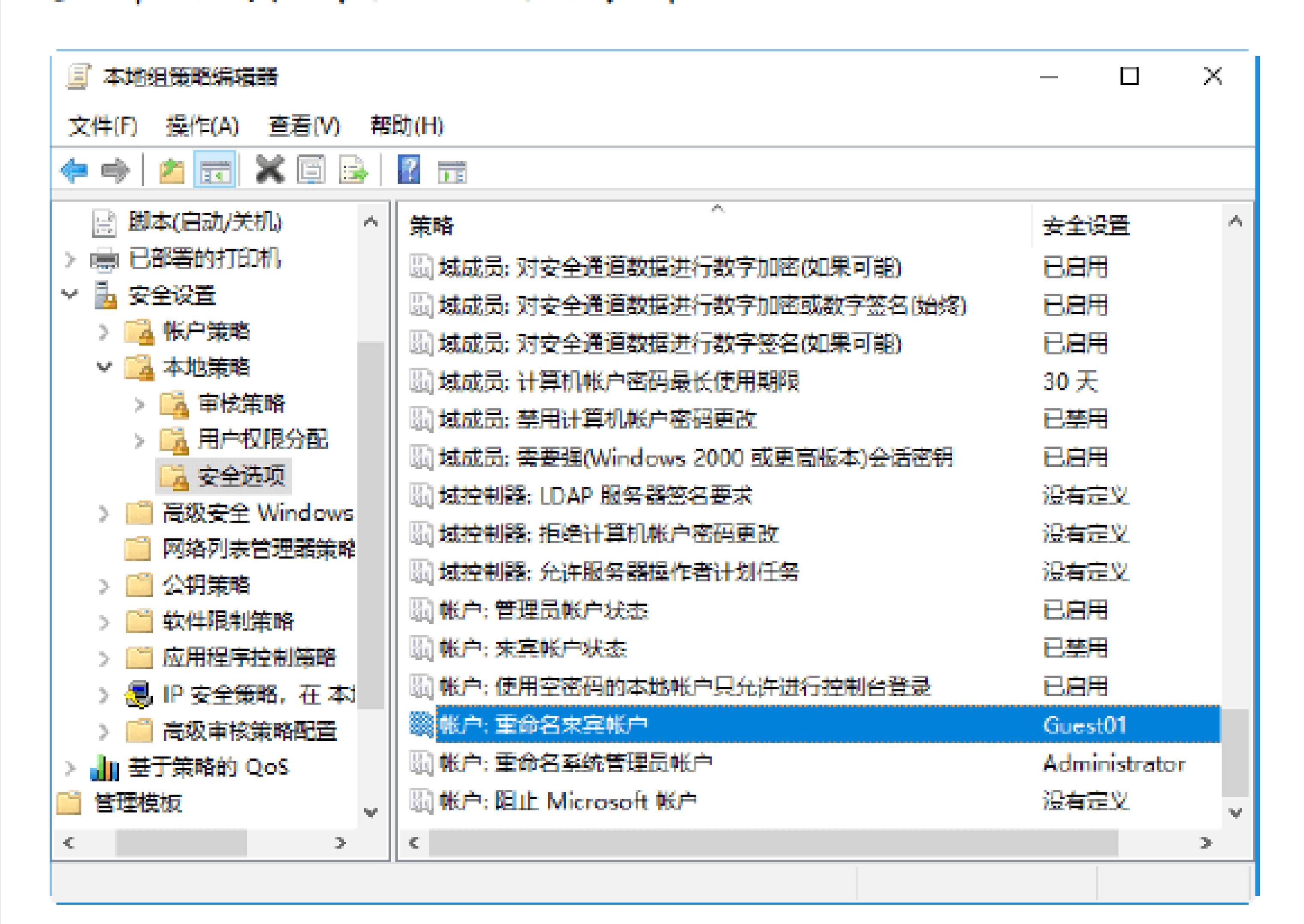
Step 03 在文本框中输入相应的名称之后，单击“确定”按钮，即可完成重命名操作，如下图所示。



Step 04 双击“账户：重命名来宾账户”选项，打开“账户：重命名来宾账户 属性”对话框，如下图所示。



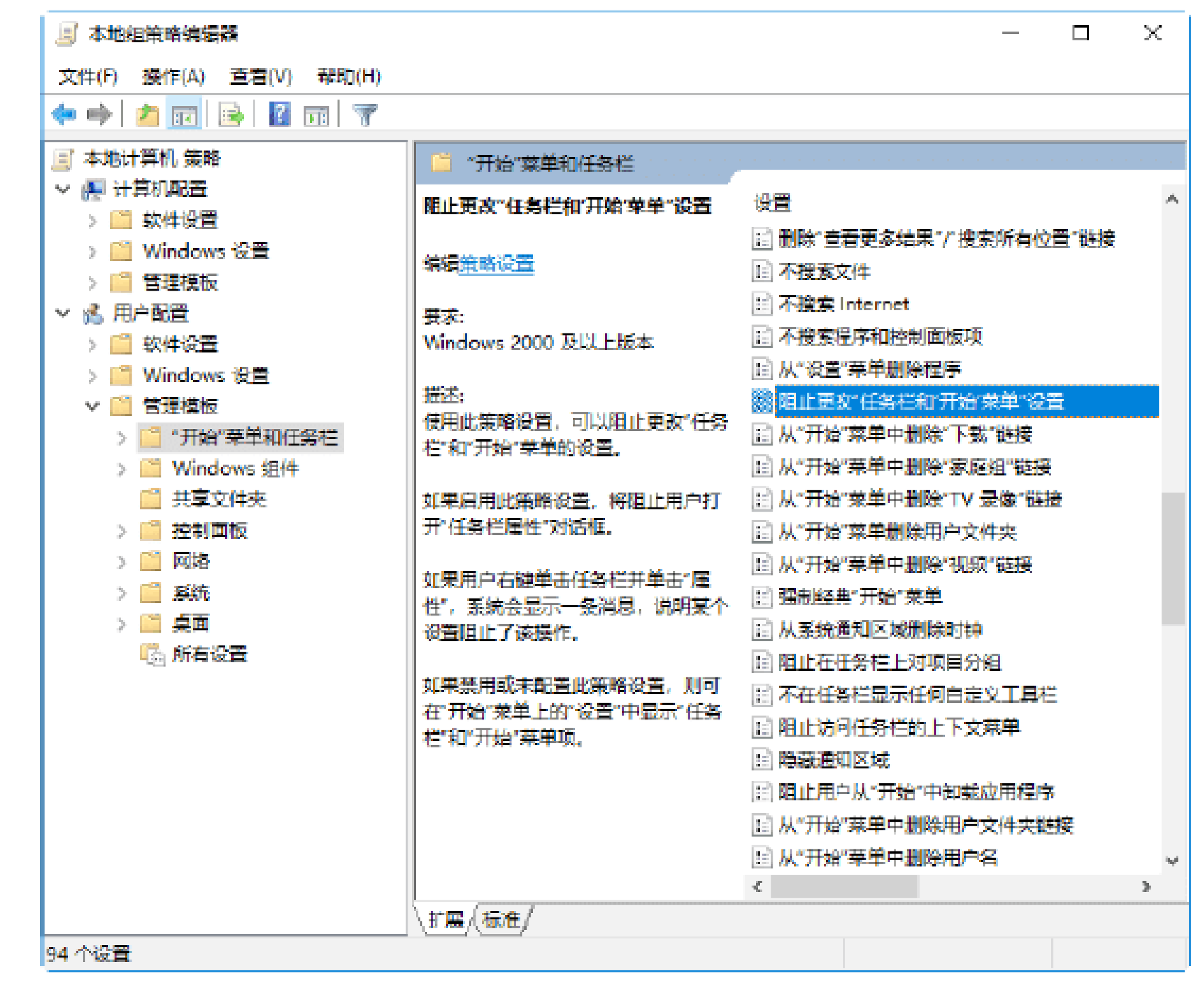
Step 05 在文本框中输入重新命名的来宾账户的名称后，单击“确定”按钮，即可完成重命名操作，如下图所示。



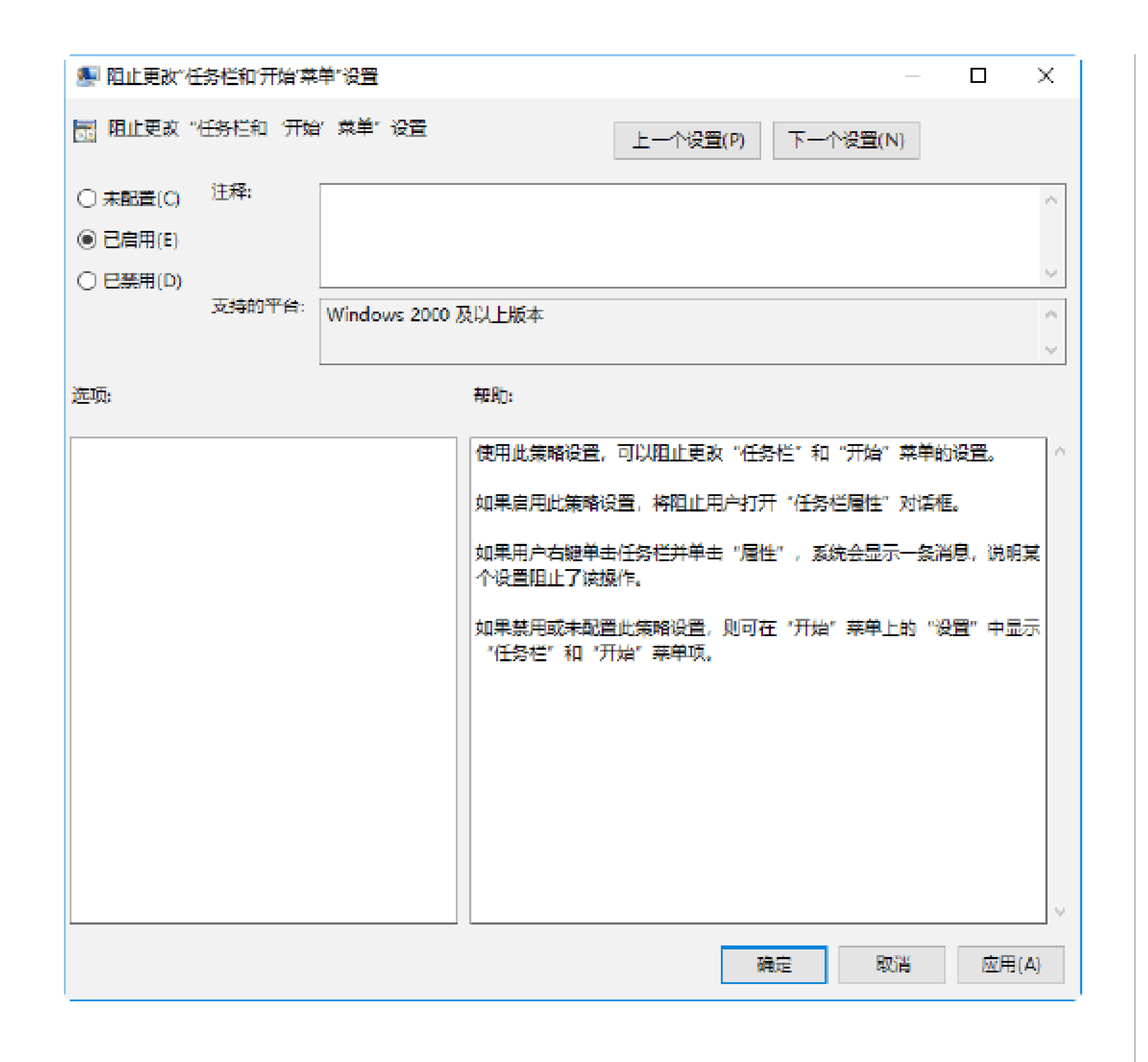
实战14：禁止更改“开始”菜单

黑客在侵入计算机时，如果随意更改“开始”菜单和任务栏，同样会给用户的正常使用带来麻烦，所以需要在组策略中将“开始”菜单和任务栏设置为禁止更改。具体操作步骤如下。

Step 01 在“本地组策略编辑器”窗口中，依次展开“用户配置”→“管理模板”→“开始菜单和任务栏”选项，即可进入“开始菜单和任务栏”窗口，如下图所示。



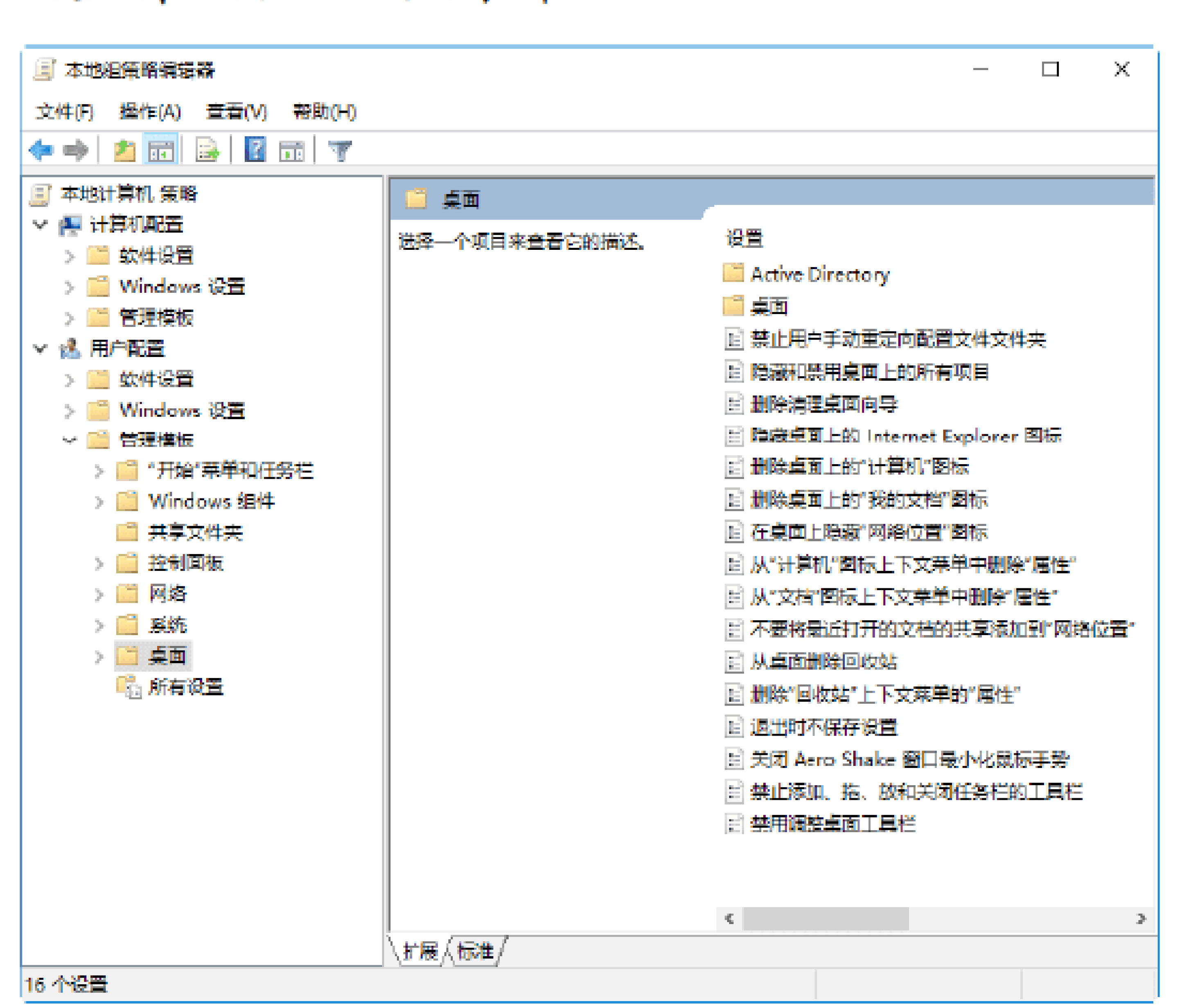
Step 02 在“设置”列表中右击“阻止更改任务栏和开始菜单设置”选项，在快捷菜单中选择“编辑”选项，打开“阻止更改任务栏和开始菜单设置”对话框，在其中选中“已启用”单选按钮后，单击“确定”按钮即可，如下图所示。



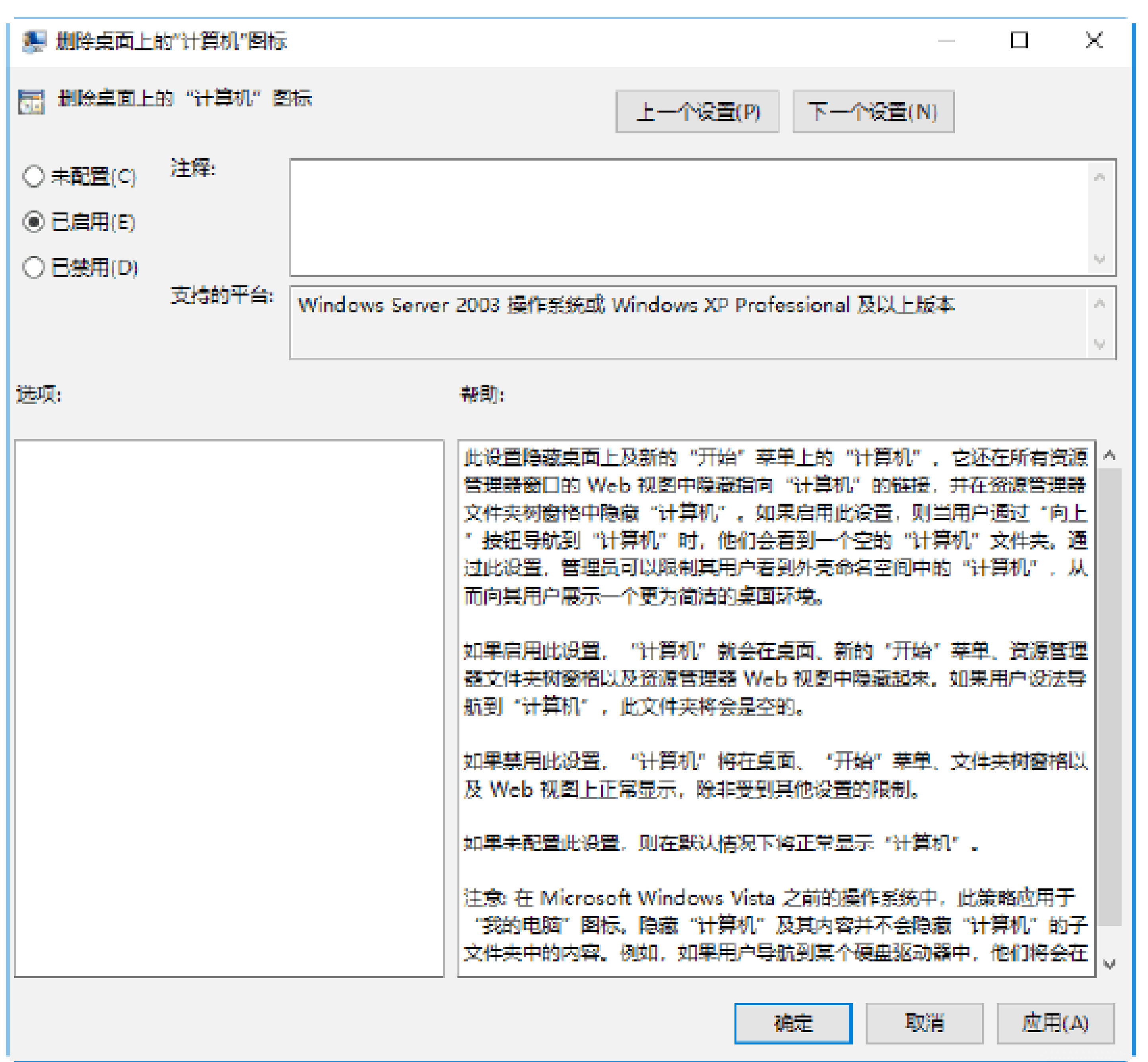
实战15：禁止更改桌面设置

桌面上一些常用软件的快捷方式可以很容易删除，但要删除“我的计算机”“回收站”“网上邻居”等系统默认图标，就需要通过“组策略”来实现，使用“组策略”可有效防止用户对桌面的某些更改。虽然通过修改注册表的方式可以实现隐藏桌面上的系统图标的功能，但这样比较麻烦，也有一定风险。而采用“组策略”配置的方法，可以方便快捷地达到此目的。具体操作步骤如下。

Step 01 在“本地组策略编辑器”窗口中，依次展开“用户配置”→“管理模板”→“桌面”选项，即可进入“桌面”设置界面，如下图所示。

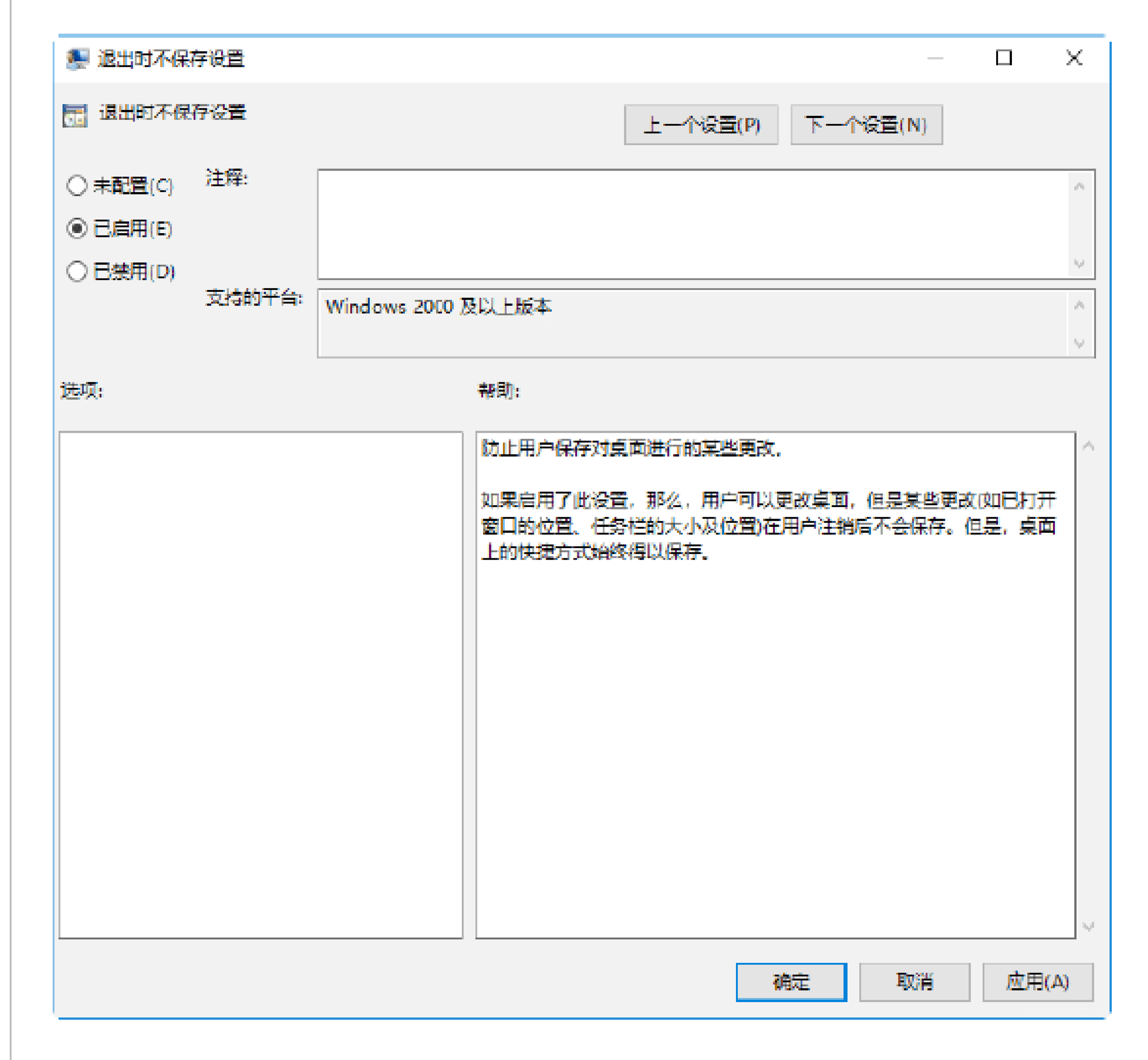


Step 02 如果要删除桌面上的“我的计算机”图标，则需要在“设置”列表中右击“删除桌面上的‘计算机’图标”选项，在快捷菜单中选择“编辑”选项，即可打开“删除桌面上的‘计算机’图标”对话框。选中“已启用”单选按钮，单击“确定”按钮，即可将计算机图标从桌面上删除。运用同样方法，即可隐藏桌面上的其他系统默认图标，如下图所示。





Step 03 要想抵制黑客的攻击，就需要启用“退出时不保存设置”功能。双击“退出时不保存设置”选项，即可打开“退出时不保存设置”对话框，选中“已启用”单选按钮，如下图所示，单击“确定”按钮，即可完成禁止对桌面进行改动。



Step 04 这样，当其他用户对桌面进行更改之后，只要重新启动计算机或实施注销操作，就可以还原到原来的设置。

13.4 使用入侵检测系统保护系统安全

通俗地讲，入侵检测（Intrusion Detection）是对入侵行为的检测。通过收集和分析网络行为、安全日志、审计入侵检测数据、网络上可以获得的信息以及计算机系统中若干关键点的信息，来检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。

入侵检测技术作为一种积极主动的安全防护技术，它提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵，可以说入侵检测技术是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护，大大提高了网络的安全水平。

一个成功的入侵检测系统，不但可以使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，而且为网络安全策略的制定提供依据。更为重要的一点是，成功的入侵检测系统应该管理、配置简单，使非专业人员也非常容易地获得网络安全。另外，入侵检测系统在发现入侵后，还应及时做出响应，包括切断网络连接、记录事件和报警等。

实战16：设置萨客嘶入侵检测系统

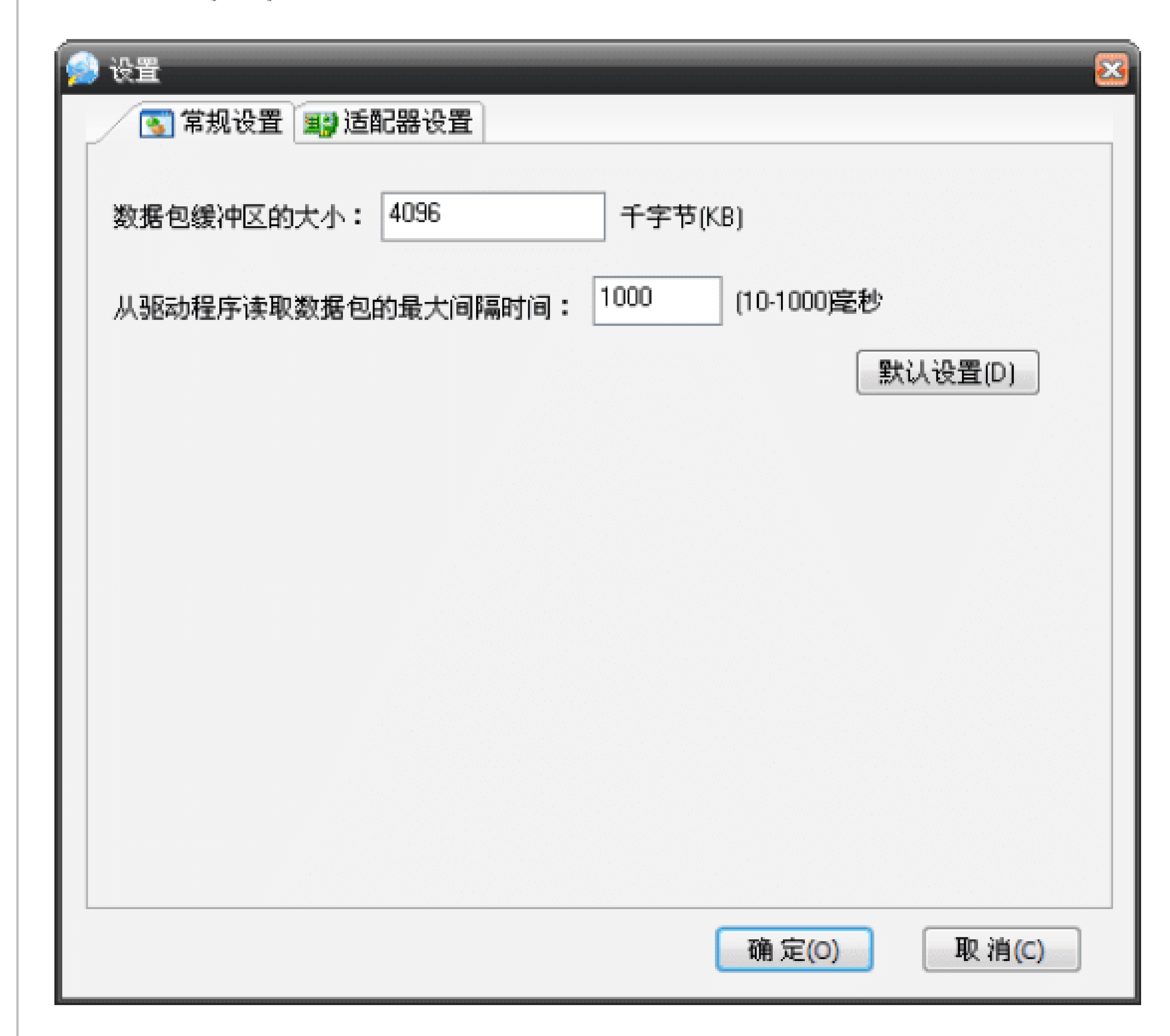
萨客嘶入侵检测系统是一种积极主动的网络安全防护工具，在使用萨客嘶入侵检测系统来防护系统或网络安全之前，还需要对该软件的相关功能进行设置，以便更好地保护系统安全。

设置萨客嘶入侵检测系统的操作步骤如下。

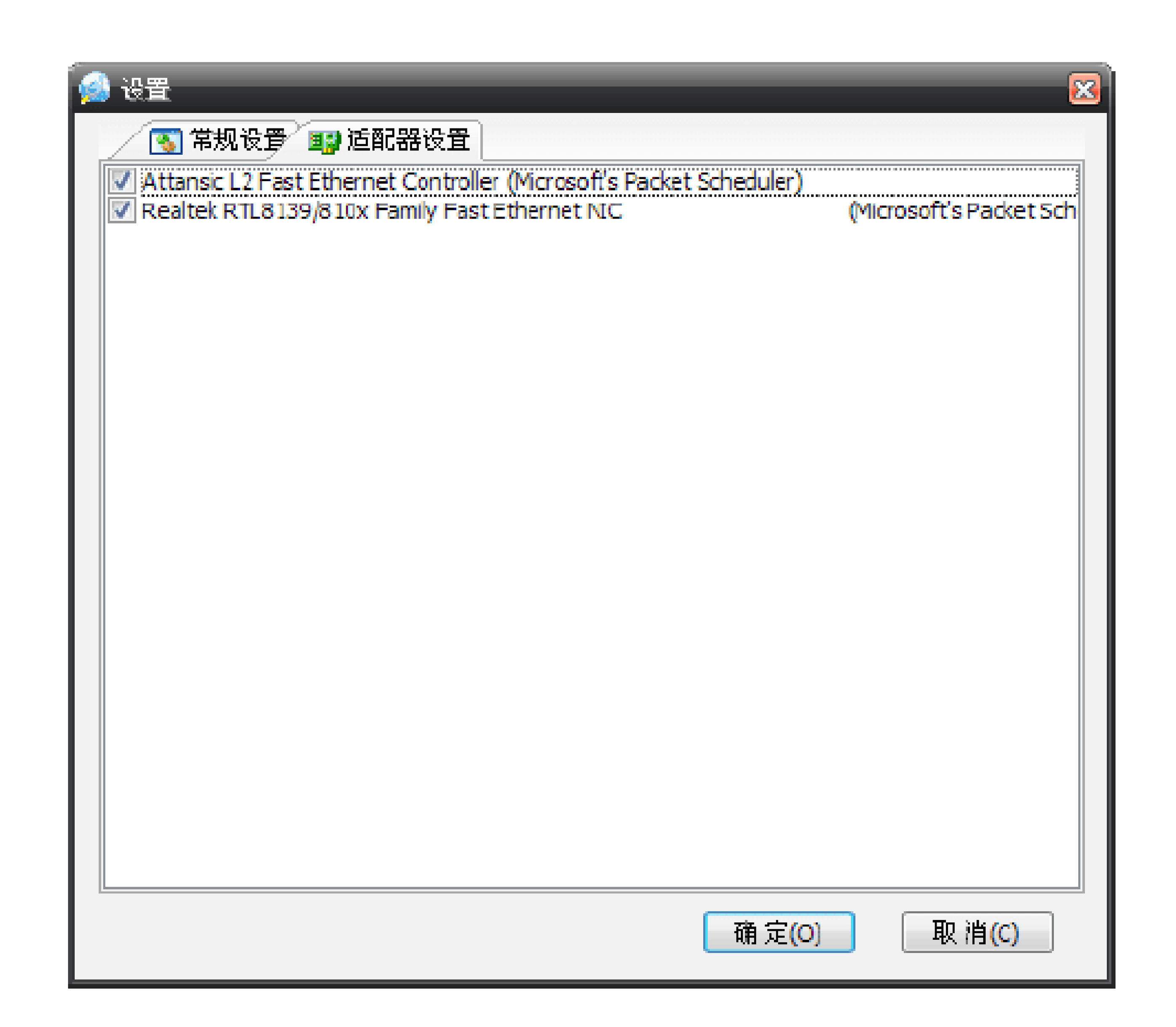
Step 01 下载并安装萨客嘶入侵检测系统，双击桌面上的快捷图标，即可打开其主界面，包括按节点浏览、运行状态以及统计项目3部分，如下图所示。



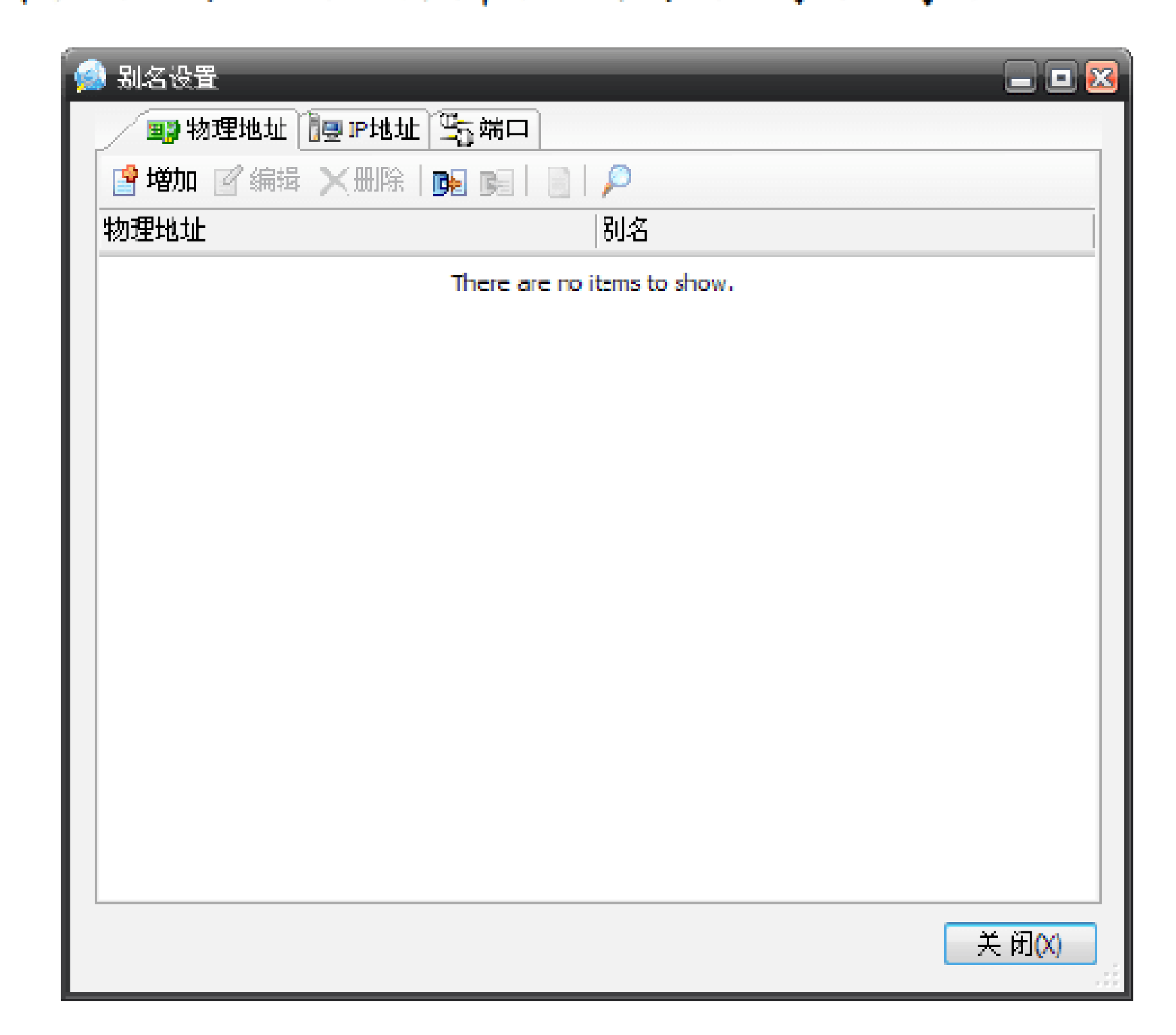
Step 02 选择“监控”→“常规设置”选项，打开“设置”对话框，在“常规设置”选项卡中可对数据包缓冲区大小和从驱动程序读取数据包的最大间隔时间进行设置，如下图所示。



Step 03 在“设置”对话框中选择“适配器设置”选项卡，即可在该选项卡中选择相应的网卡，如下图所示，因为该检测系统是通过适配器来捕捉网络中正在传输的数据，并对其进行分析，所以正确选择网卡是能够捕捉到入侵的关键点。



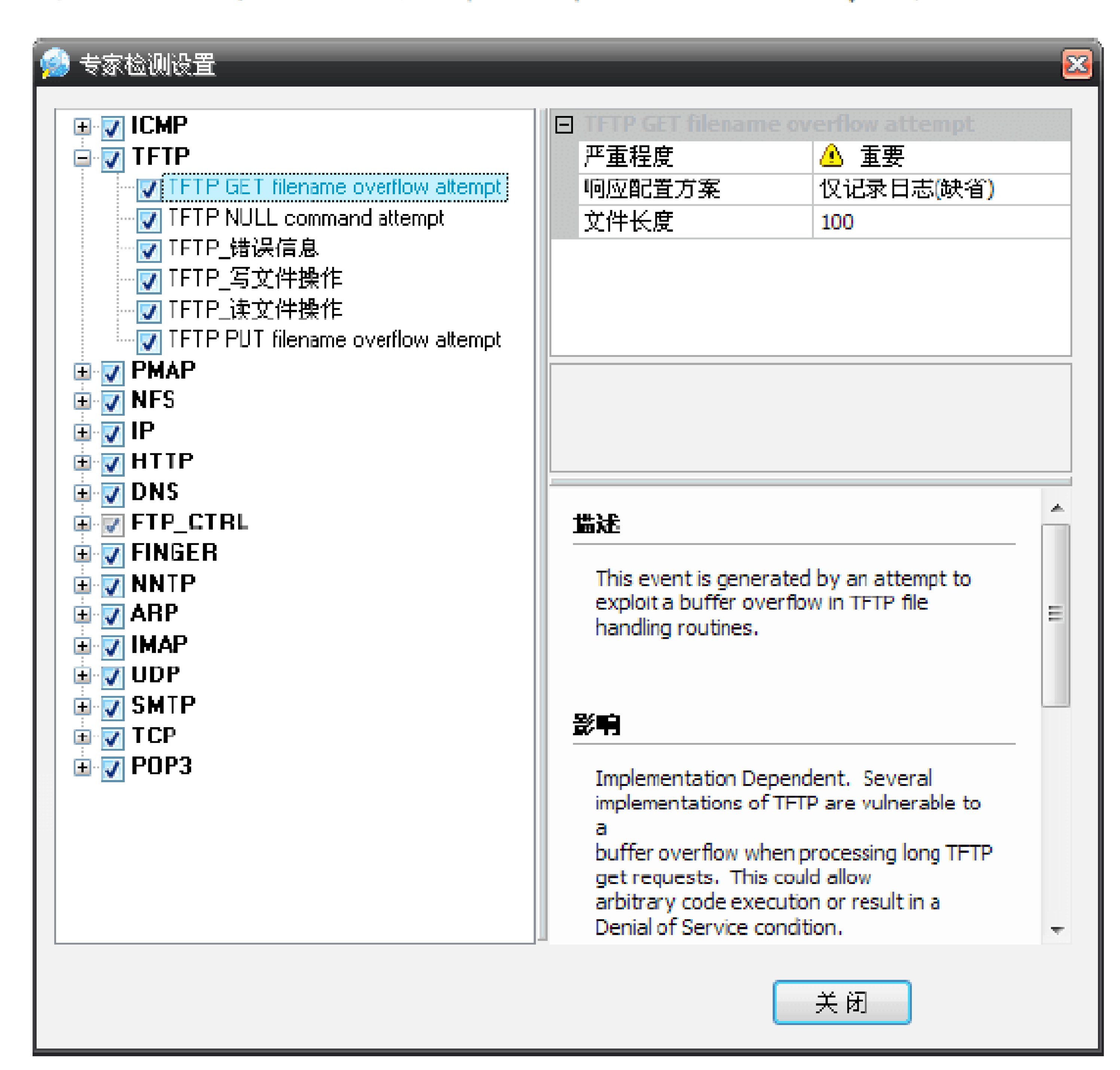
Step 04 在“萨客嘶入侵检测系统”主界面中选择“设置”→“别名设置”选项，打开“别名设置”对话框，如下图所示，在其中可对物理地址、IP地址、端口进行各种操作，如添加、编辑、删除、导出等。



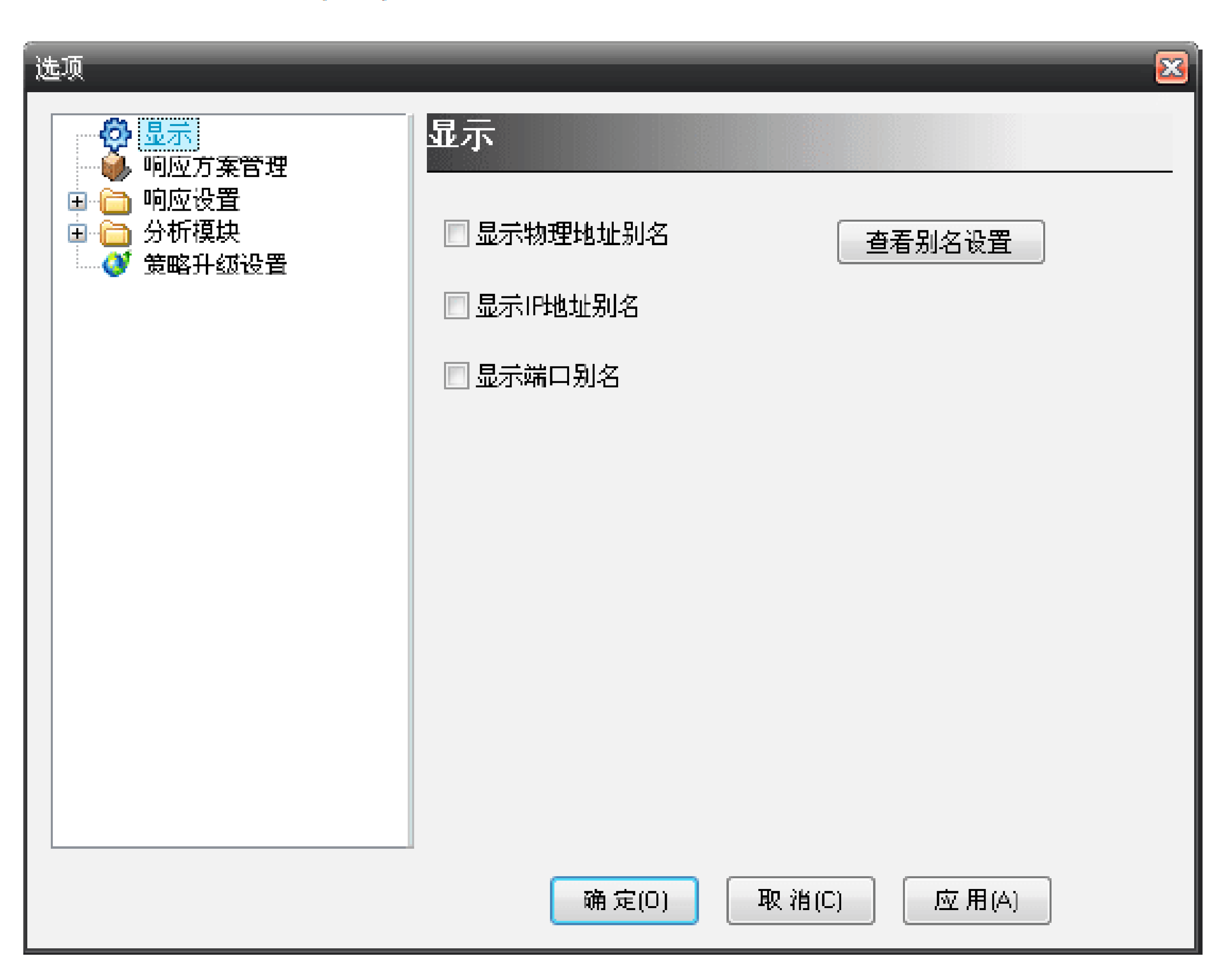
Step 05 选择“设置”→“安全策略设置”选项或单击工具栏中的“安全策略”按钮，打开“安全策略”对话框，如下图所示，即可对当前选中的策略进行相应的操作，如衍生、查看、启用、删除、导入、导出和升级等。



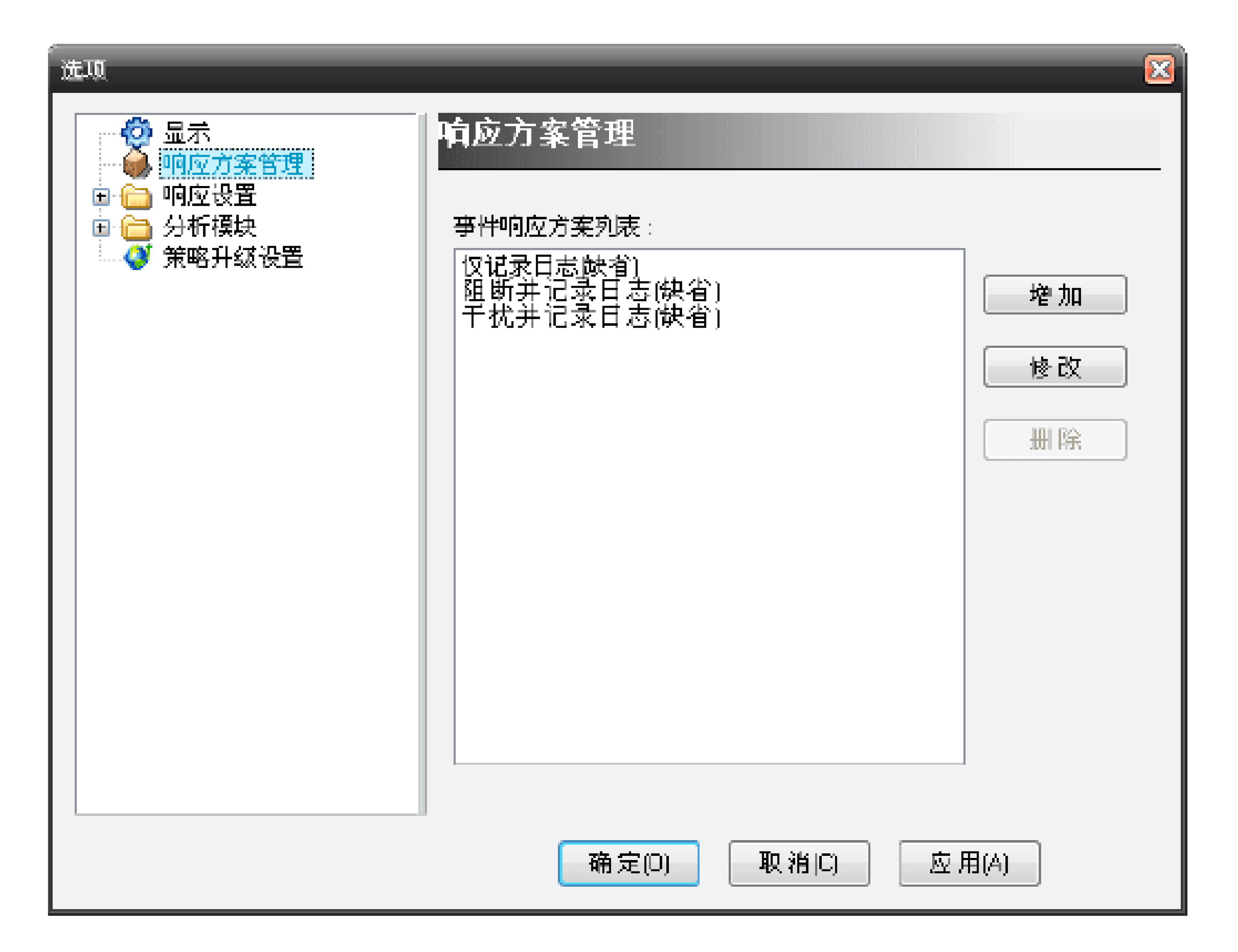
Step 06 选择“设置”→“专家检测设置”选项或单击工具栏中的“专家检测”按钮，打开“专家检测设置”对话框，如下图所示，即可对网络中的所有通信数据进行专家级的智能化分析，并报告入侵事件。



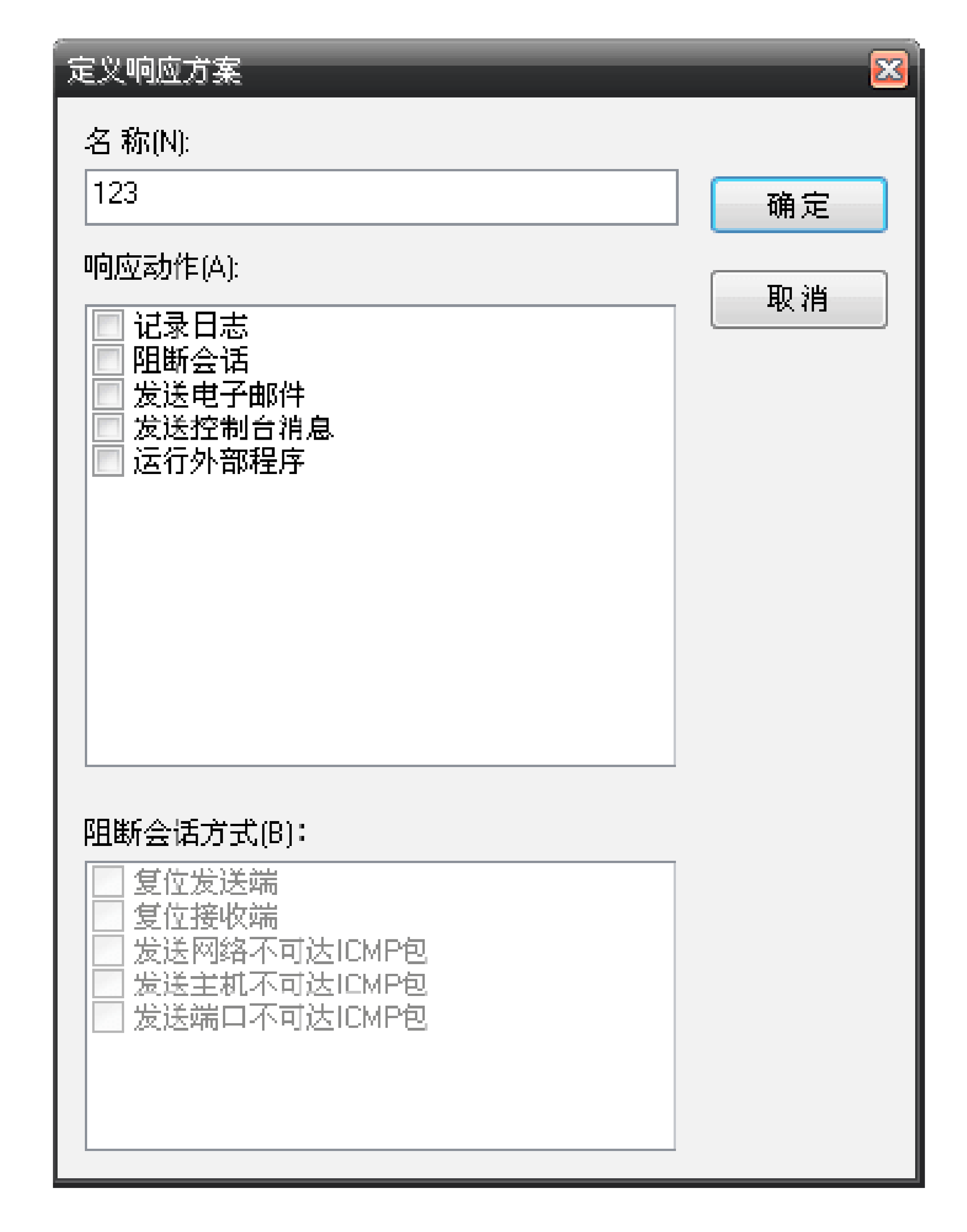
Step 07 选择“设置”→“选项”选项或单击工具栏中的“选项”按钮，打开“选项”对话框，选择“显示”功能项，即可对是否启用网卡地址、IP地址和端口别名进行设置，如下图所示。



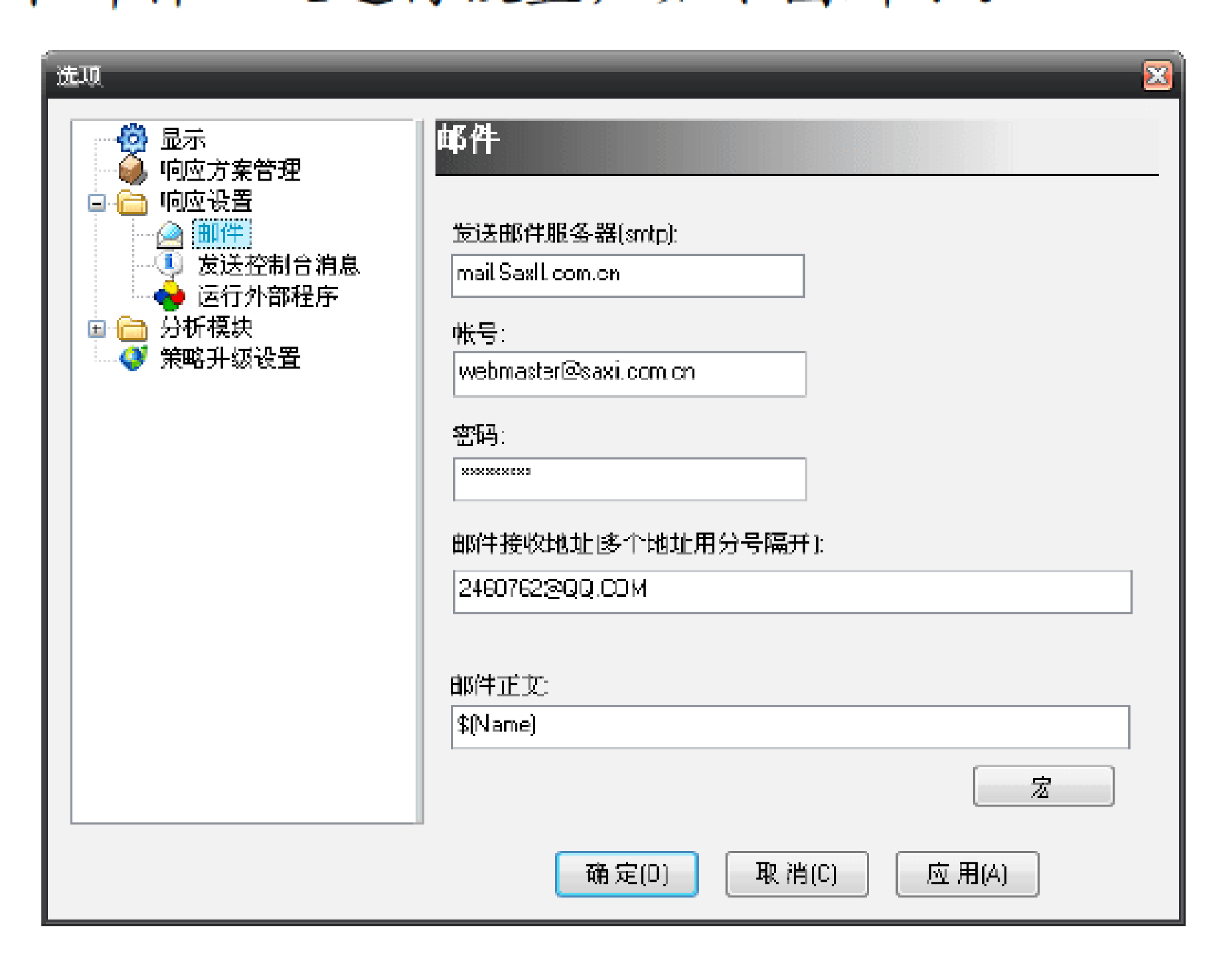
Step 08 选择“响应方案设置”选项，即可对响应方案进行增加、删除或修改操作，如下图所示。系统提供了“仅记录日志”“阻断并记录日志”和“干扰并记录日志”3种缺省的响应方案，它们是不能被删除的，但是可以修改。



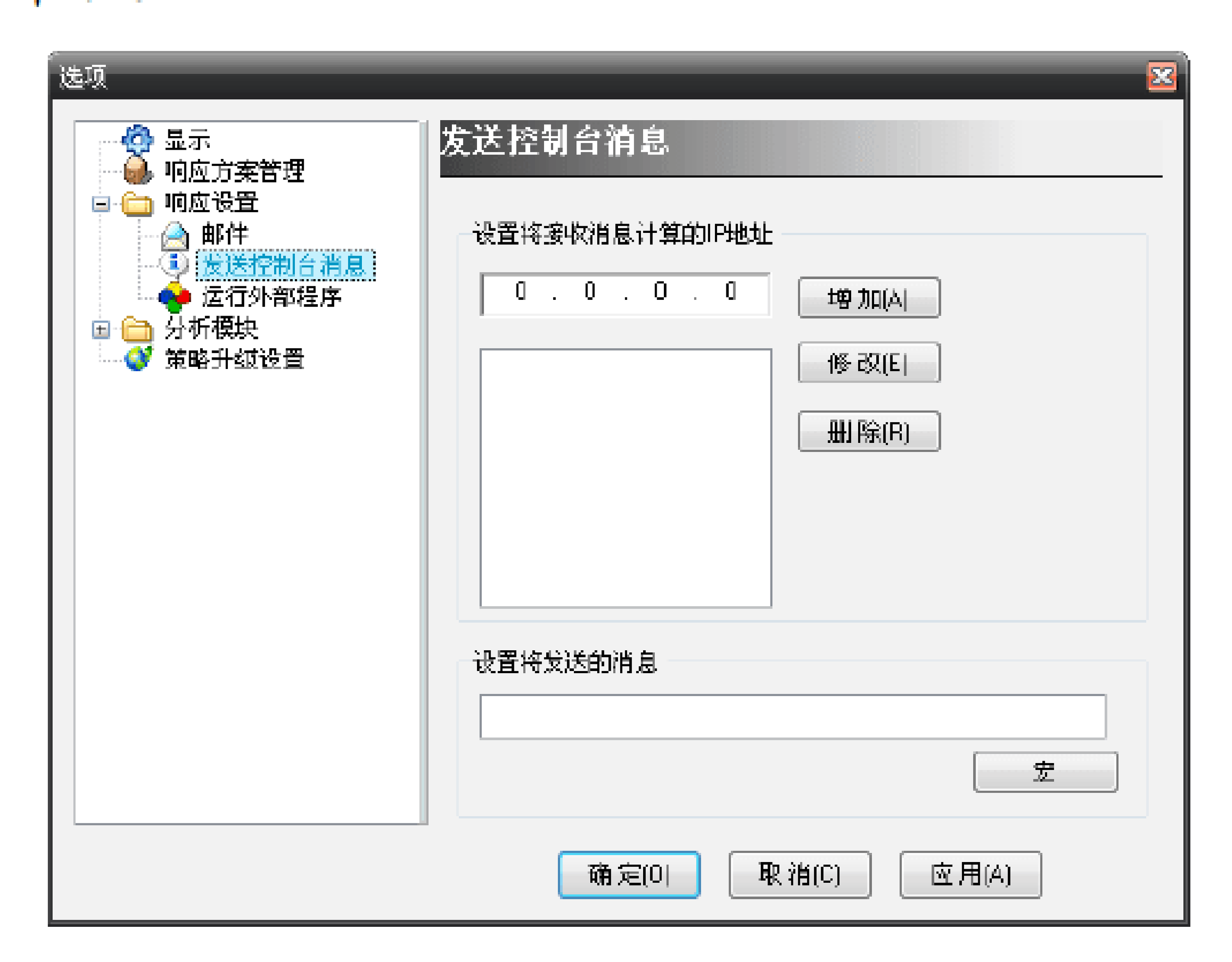
Step 09 单击“增加”或“修改”按钮，打开“定义响应方案”对话框，如下图所示，即可对响应方案进行具体设置，包括名称、响应动作和阻断会话方式（只有选择了“阻断会话”才可以设置“阻断会话方式”）。



Step 10 选择“响应设置”→“邮件”选项，即可对发送邮件所使用的服务器、账号、密码、接收地址（多个地址用分号分隔）和邮件正文进行设置，如下图所示。



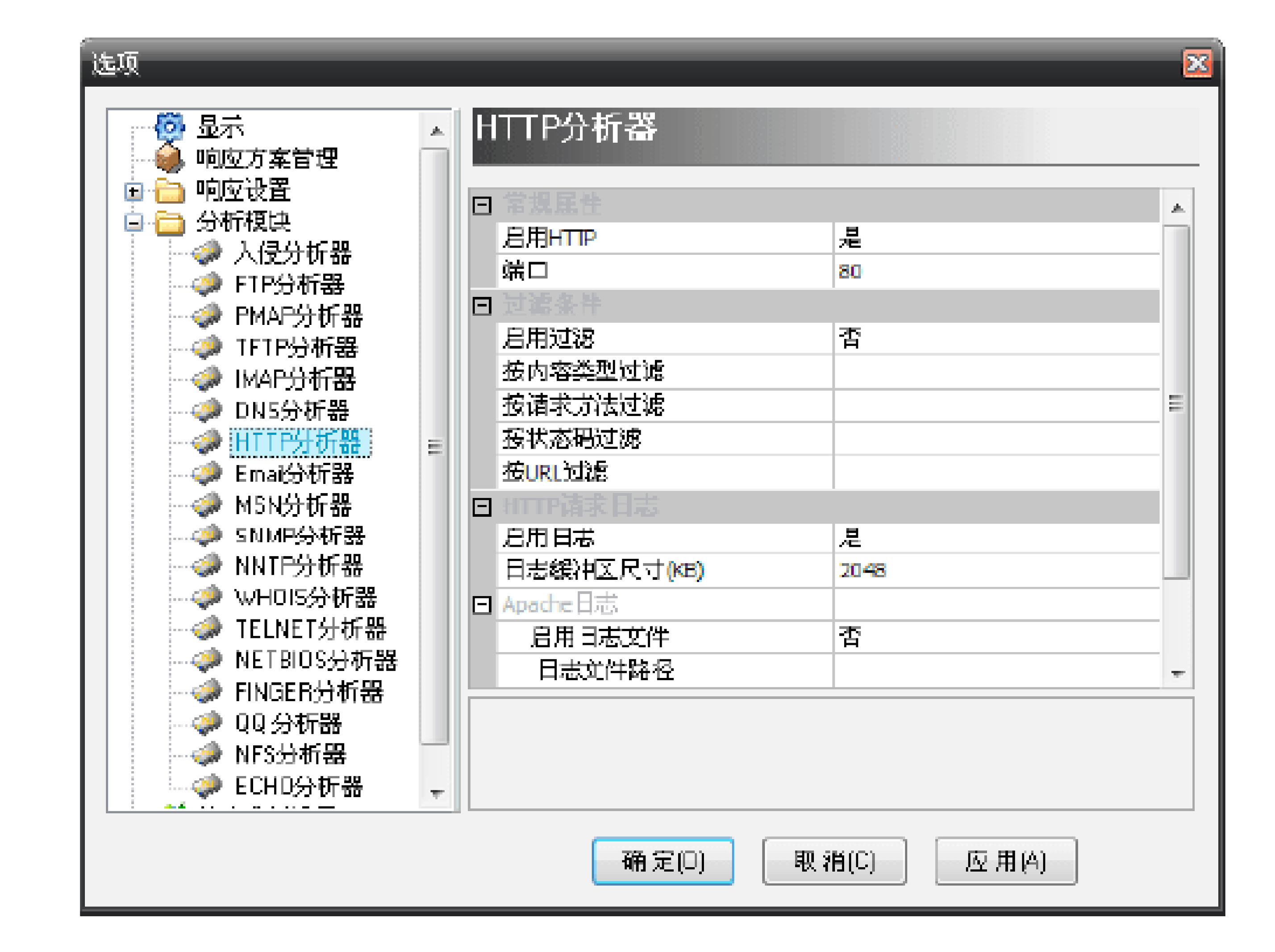
Step 11 选择“响应设置”→“发送控制台消息”选项，即可对接收消息的目标主机的IP地址和消息正文（发送主机和接收主机必须安装Messenger服务）进行设置，如下图所示。



Step 12 选择“响应设置”→“运行外部程序”选项，即可对外部程序的完整路径和参数进行设置，如下图所示。



Step 13 选择“分析模块”选项，即可对各个分析模块的参数进行个性化的设置，如是否启用该分析模块、检测的端口、日志缓冲区的大小、是否保存日志等，如下图所示。



Step 14 选择“策略升级设置”选项，即可通过定时和手工两种方式检测策略知识库，更新萨客嘶入侵检测系统，并自动完成对本地知识库的更新，如下图所示。如果选择自动更新，还必须设置更新的日期和时间，在所有选项设置完成后，单击“确定”按钮，即可保存设置。

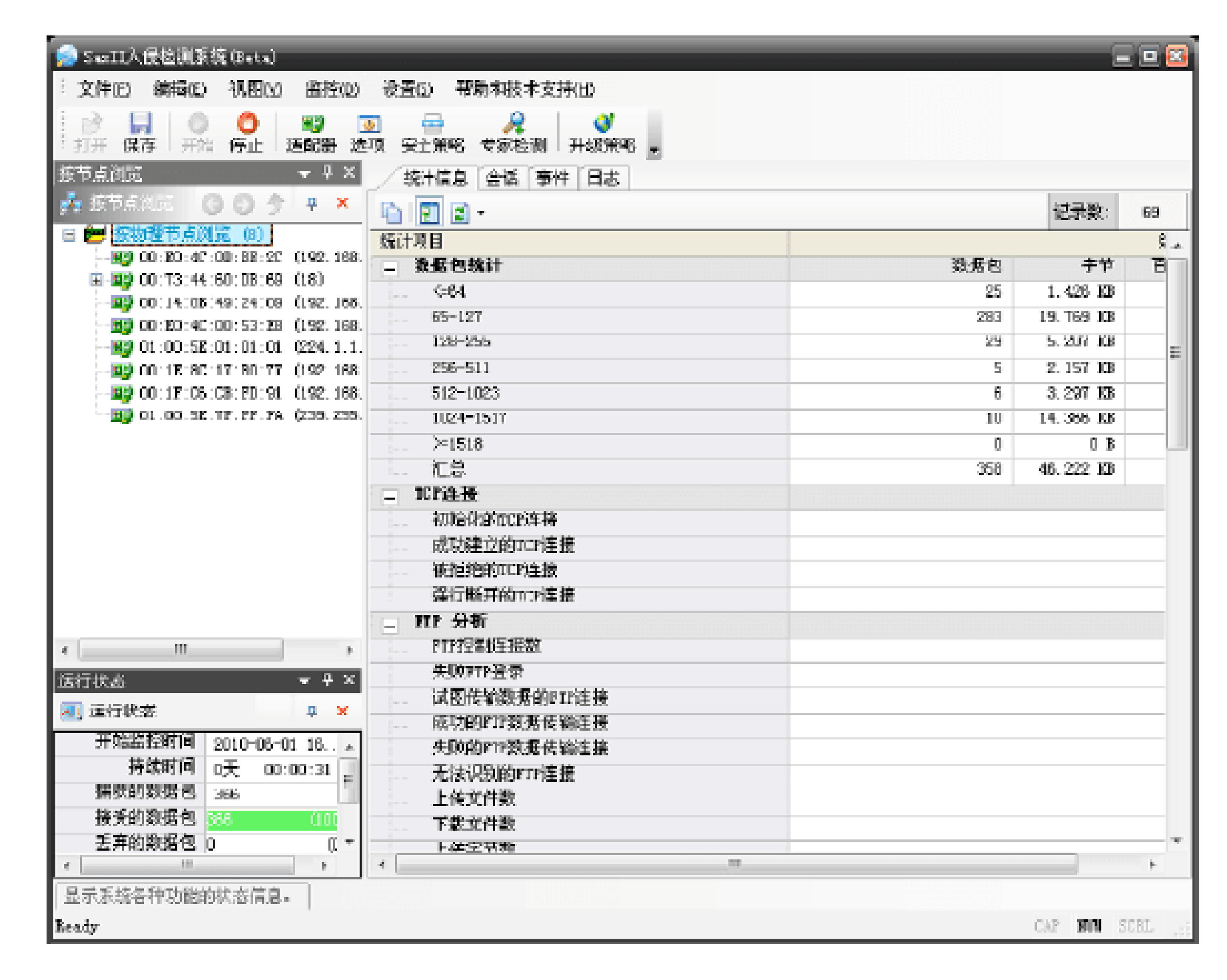


实战17：使用萨客嘶入侵检测系统

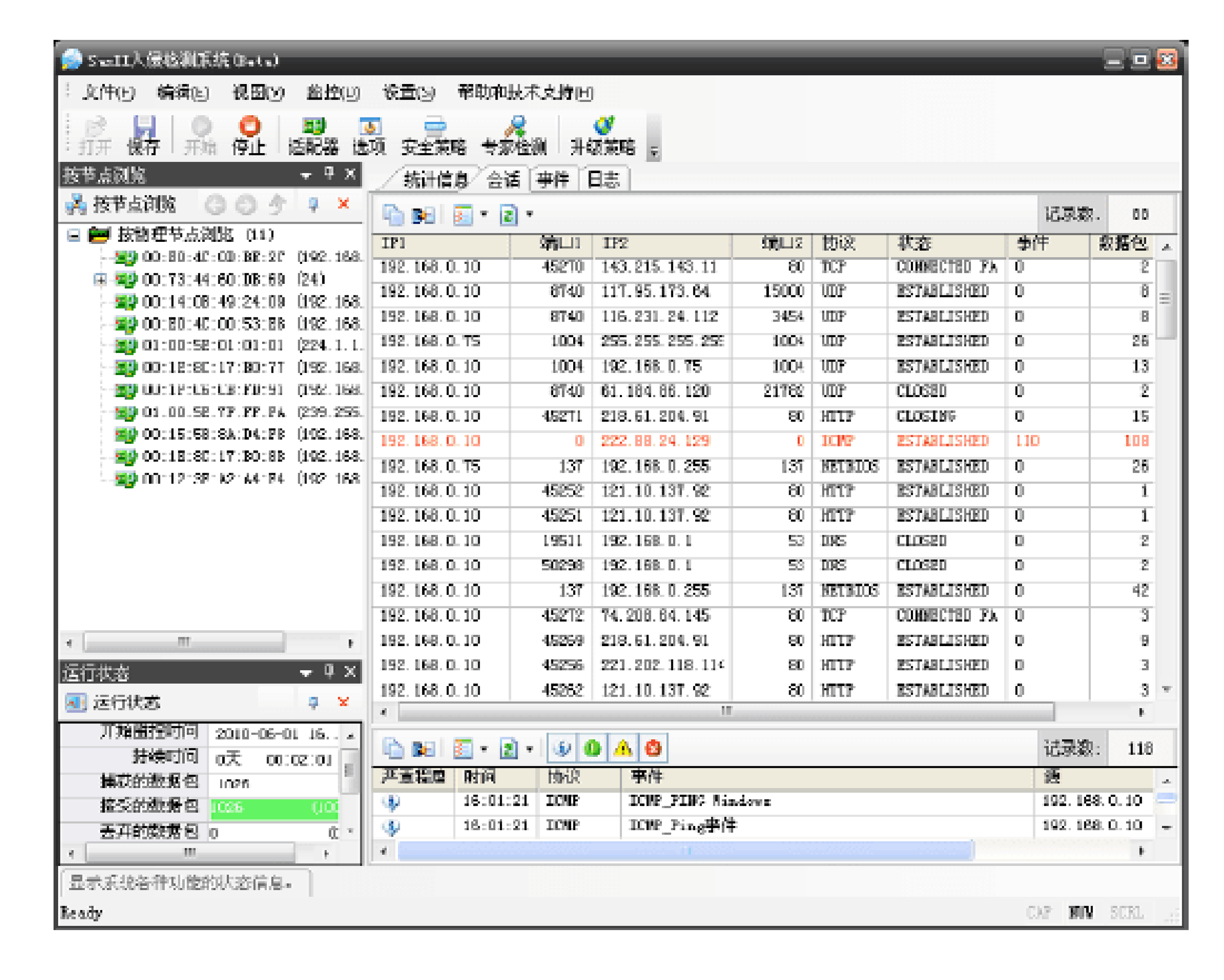
萨客嘶入侵检测系统提供了对内部和外部攻击的实时保护，它通过对网络中所有传输的数据进行智能分析和检测，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象，在网络系统受到危害之前拦截和阻止入侵。

使用萨客嘶入侵检测系统防护网络或本机系统安全的具体操作步骤如下。

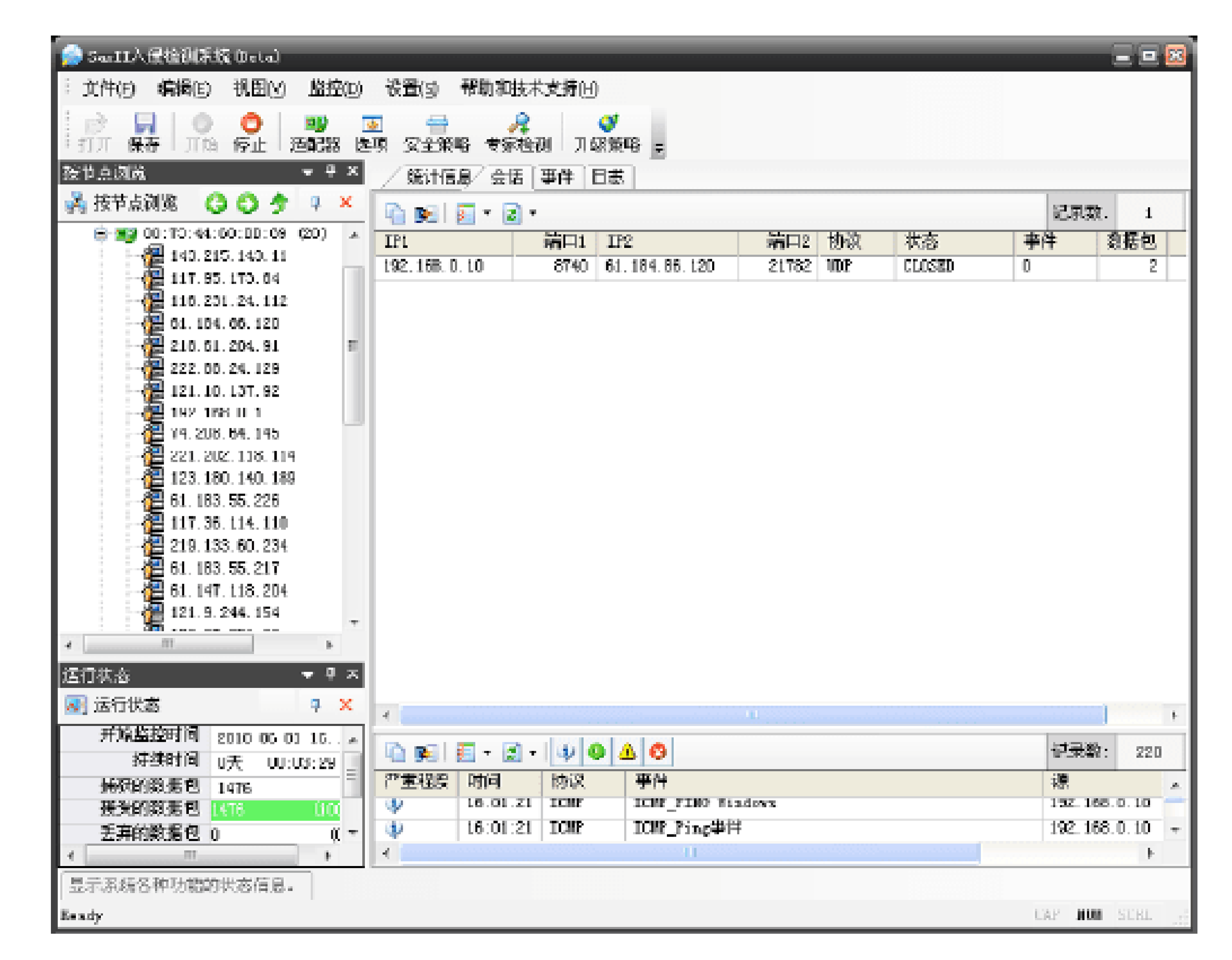
Step 01 在“萨客嘶入侵检测系统”主窗口中，单击“开始”按钮或选择“监控”→“开始”选项，即可对本机所在的局域网中的所有主机进行监控，在扫描结果中可对检测到的主机的IP地址、对应的MAC地址、本机的运行状态以及数据包统计、TCP连接情况、FTP分析等信息进行查看，结果如下图所示。



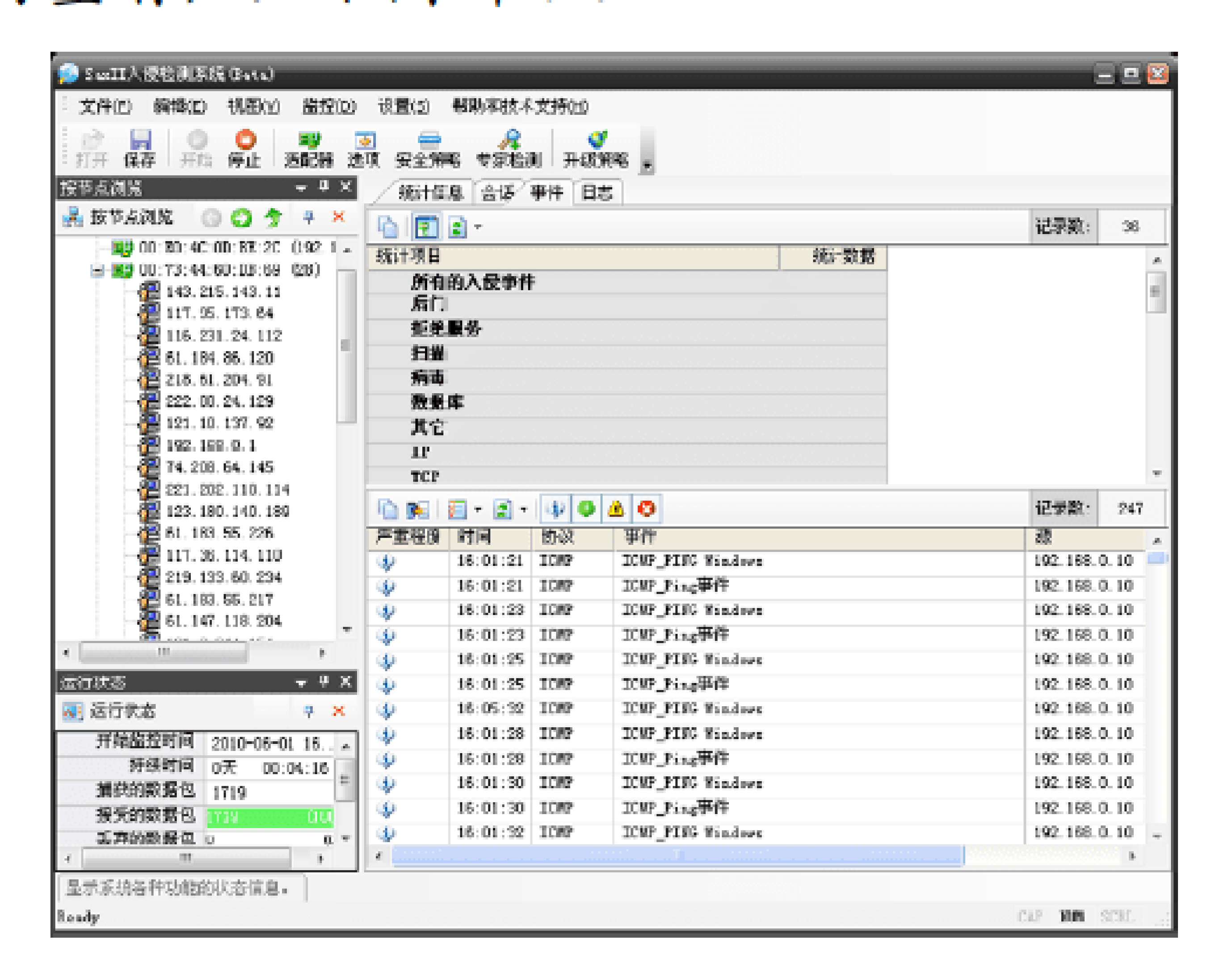
Step 02 选择“会话”选项卡，在其中可以看到在监控的同时进行会话的源IP地址、源端口、目标IP地址、目标端口、使用到的协议类型、状态、事件、数据包、字节等信息，如下图所示。



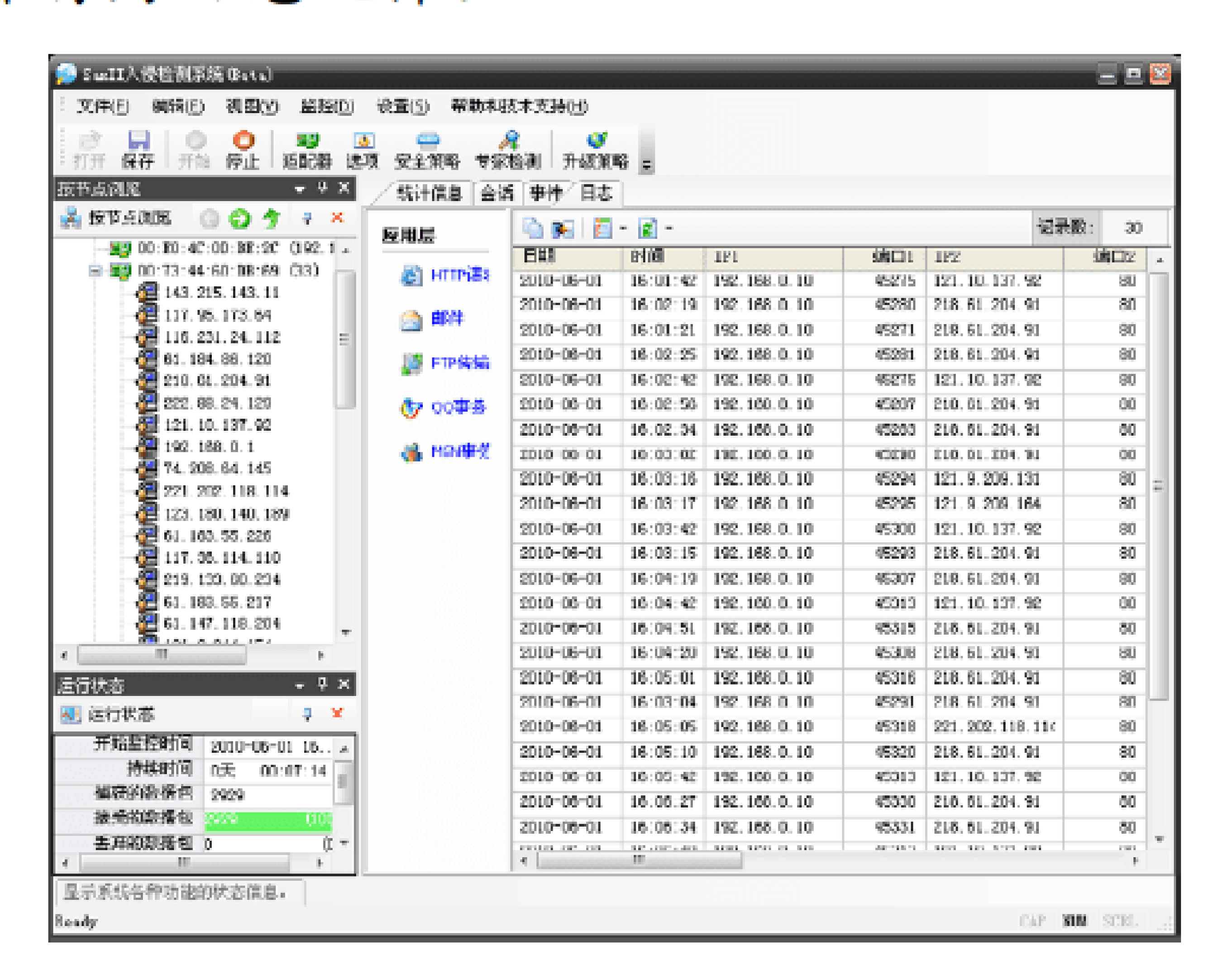
Step 03 如果想分类查看会话信息，则在“会话信息”列表中右击某条信息，在弹出的快捷菜单中选择“按目标节点进行过滤”选项，即可以按照某个目标IP地址来显示会话信息，如下图所示。



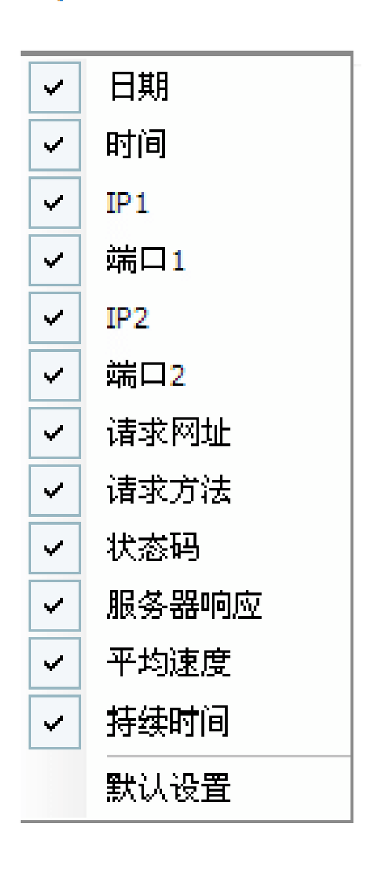
Step 04 选择“事件”选项卡，在该选项卡中即可对分类统计的各种入侵事件次数、采用日志详细记录的入侵时间、发起入侵的计算机、严重程度、采用的方式等信息进行查看，如下图所示。



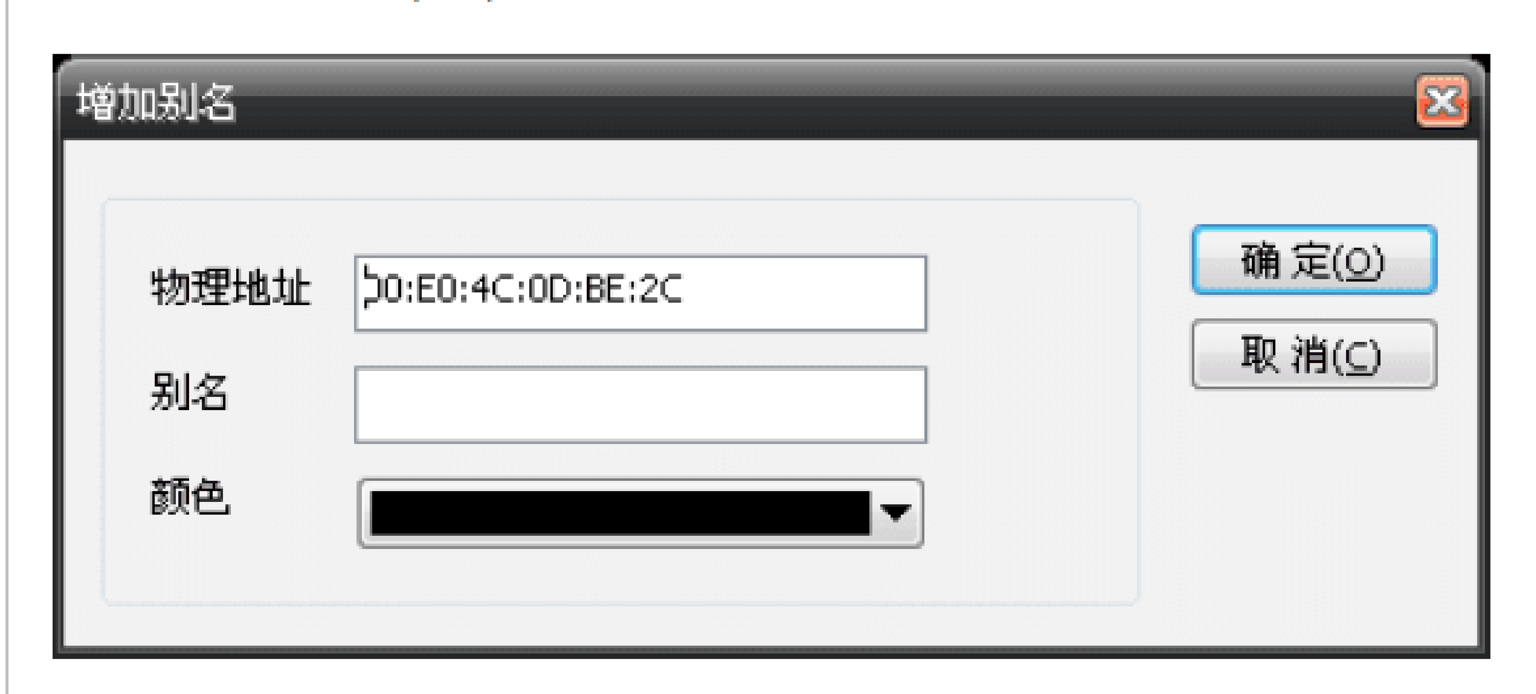
Step 05 选择“日志”选项卡，在其中记录了HTTP请求、收发邮件信息、FTP传输和MSN和QQ通讯等相关信息，如下图所示，除了对这些信息进行查看外，还可以将其保存为日志文件。



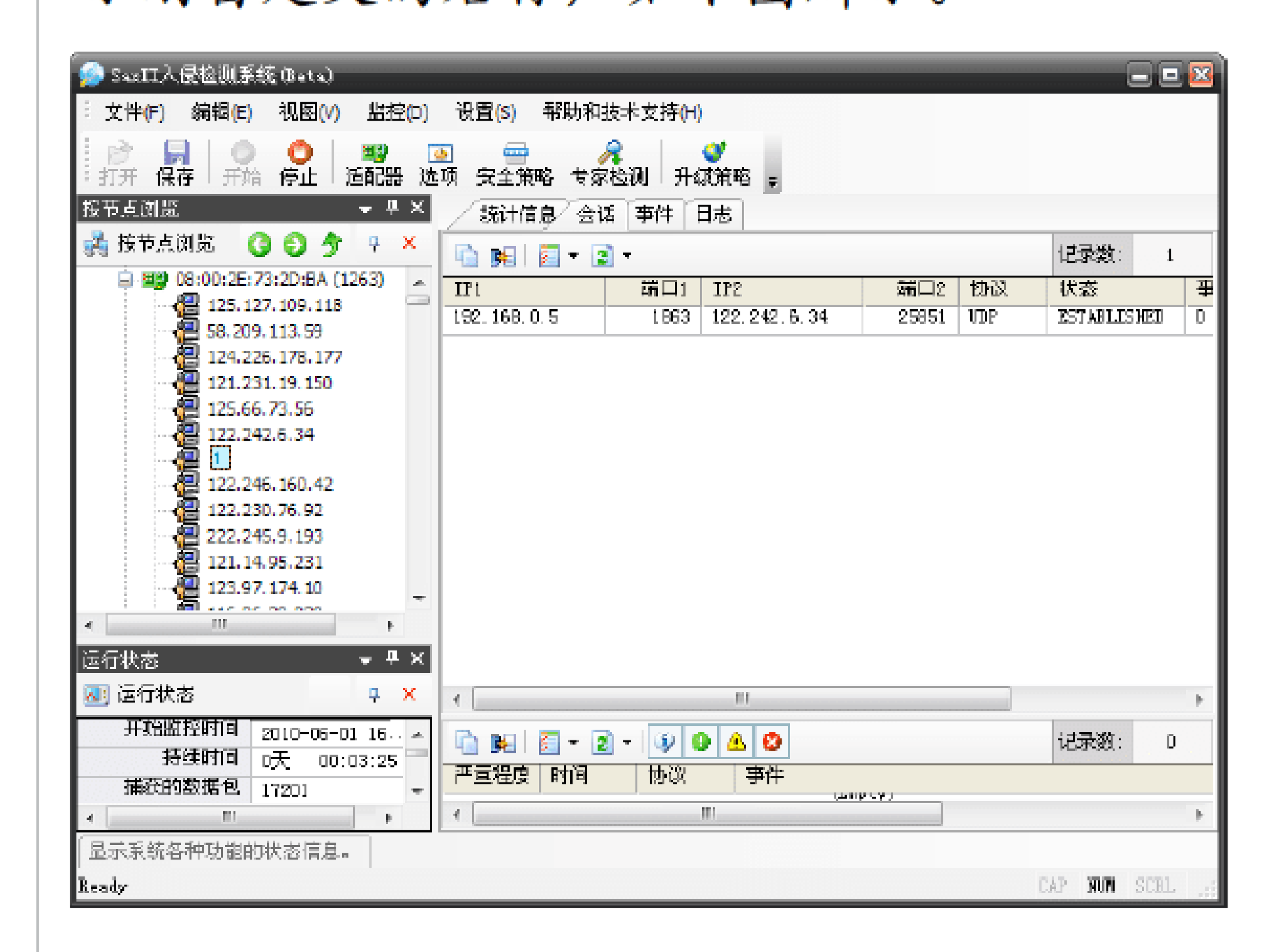
Step 06 在“日志”选项卡下可自行定义日志的显示格式，单击“自定义列”按钮 ，在打开的快捷菜单中取消勾选相应的复选框即可，如下图所示。



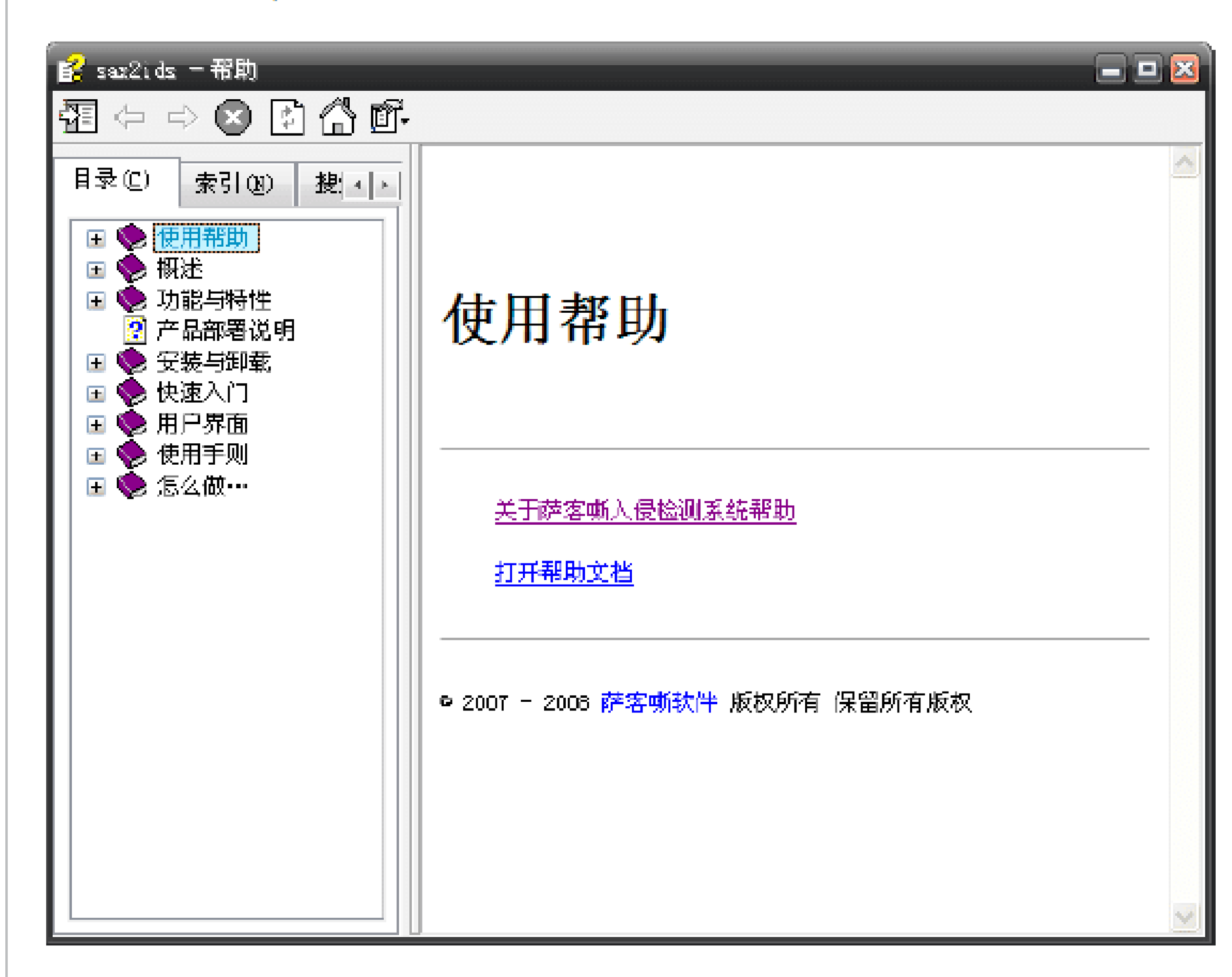
Step 07 在左边的节点列表中右击某个物理地址，在弹出的快捷菜单中选择“增加别名”选项，即可打开“增加别名”对话框，如下图所示。



Step 08 在“别名”文本框中输入名称，然后单击“确定”按钮，即可使该物理地址显示刚自定义的名称，如下图所示。



Step 09 用户在遇到不能解决的问题时，可选择“帮助和技术支持”→“帮助主题”选项，在打开的“帮助”窗口中查找所需要的问题解答，如下图所示。

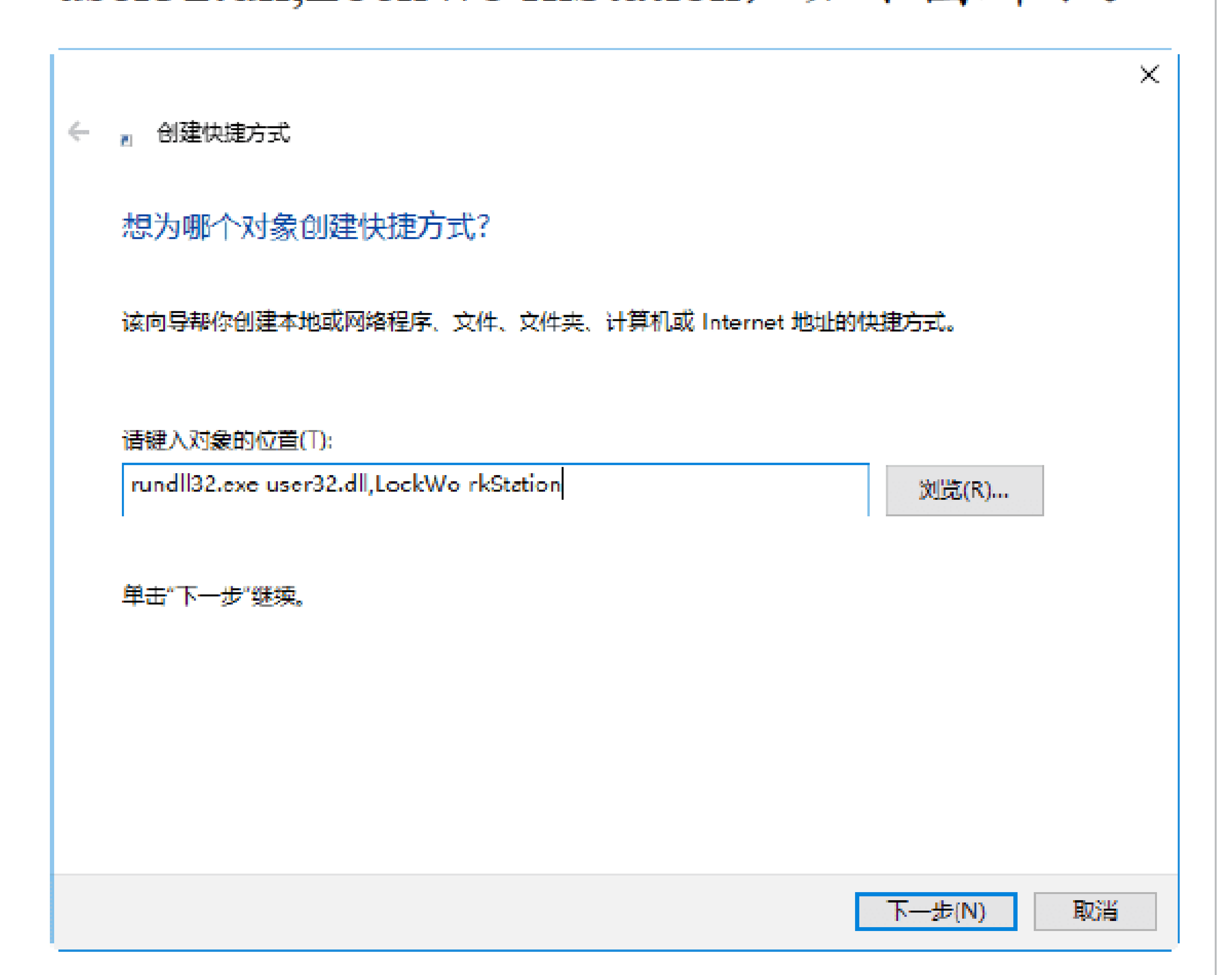


13.5　实战演练

实战演练1——一键锁定计算机

频繁地对计算机进行开关机等操作，会对计算机带来不利的影响，但在实际工作过程中难免会出现需要暂时离开的情况，此时可以通过将计算机锁定起来，就可以放心地离开而又不用进行关机。锁定计算机的具体步骤如下。

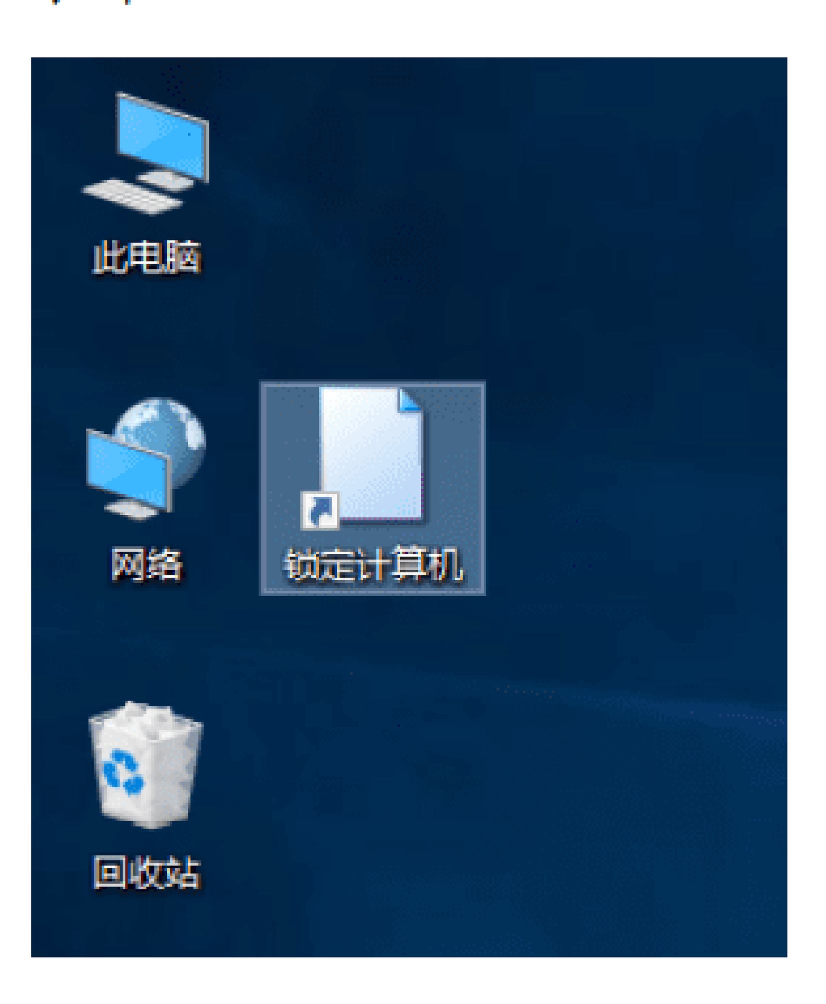
Step 01 在计算机桌面上右击鼠标，在快捷菜单中选择“新建”→“快捷方式”选项，打开“创建快捷方式”对话框，在“请键入对象的位置”文本框中输入rundll32.exe user32.dll,LockWo rkStation，如下图所示。



Step 02 单击“下一步”按钮，在打开的对话框的“键入该快捷方式的名称”文本框中输入快捷方式名称，如下图所示。

Step 03 单击“完成”按钮，即可完成设置操作，此时桌面上就出现了该快捷方式图标，如下图所示。



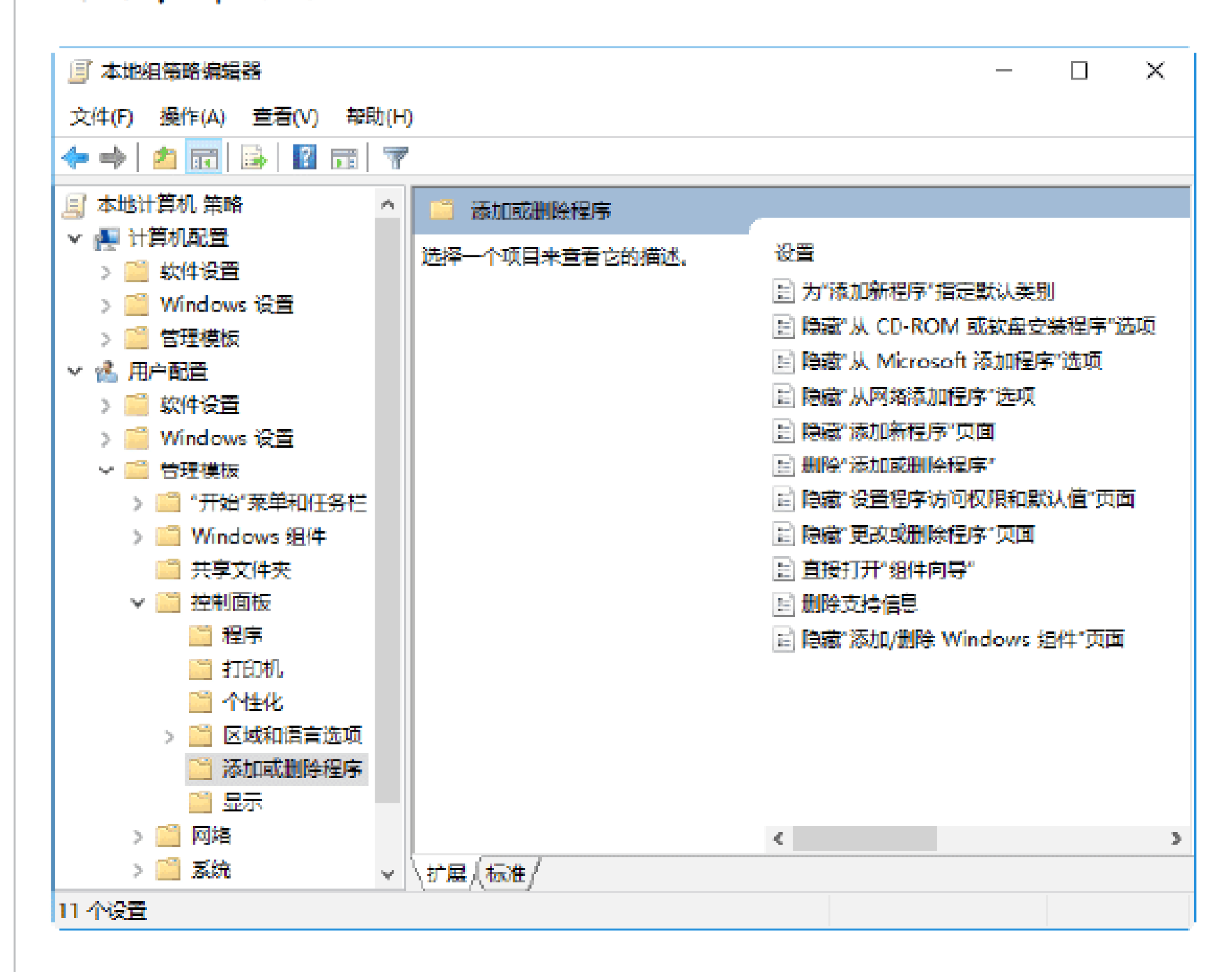


Step 04 用户只需在离开时双击此图标，即可将计算机锁定起来。如果想再次进入系统，就需要在登录界面中输入用户的账号密码，可以起到很好的保护作用。

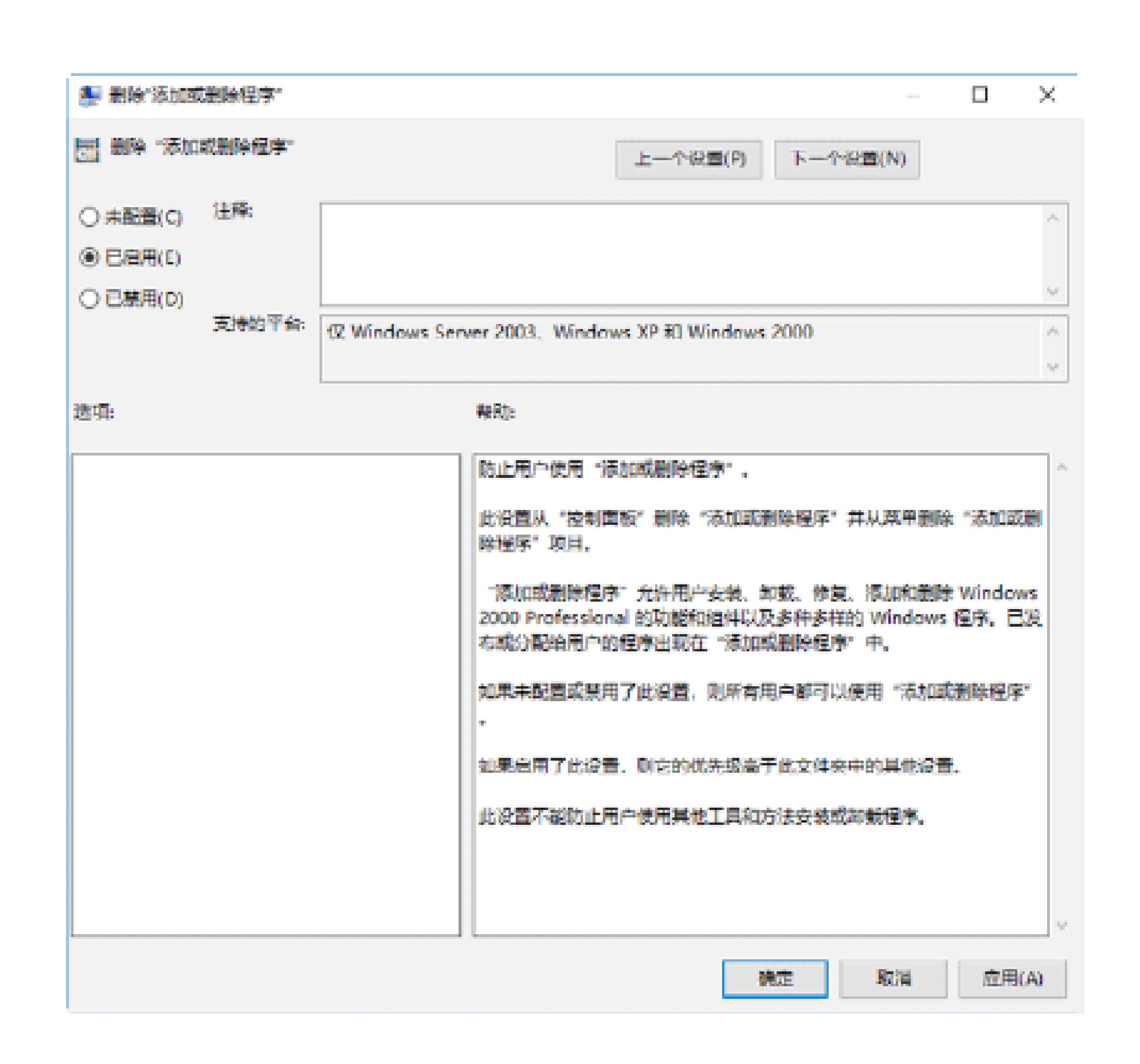
实战演练2——禁用“添加或删除程序”

黑客在入侵计算机之后，往往喜欢通过“添加或删除程序”操作来删除本计算机中的重要应用程序而实现入侵。所以最好在“组策略”窗口中启用“删除‘添加或删除程序’”功能。具体操作步骤如下。

Step 01 在“本地组策略编辑器”窗口中依次展开“用户配置”→“管理模板”→“控制面板”→“添加或删除程序”选项，即可进入“添加或删除程序”设置界面，如下图所示。



Step 02 双击“删除‘添加或删除程序’”选项，打开“删除‘添加或删除程序’”对话框，选中“已启用”单选按钮，如下图所示。



Step 03 单击“确定”按钮，即可自动把“添加或删除程序”选项从“控制面板”窗口中删除，此程序也会从“开始”菜单中删除。

注意：这种方法只能阻止通过“添加或删除程序”实现的软件安装、卸载操作，并不能防止用户使用其他工具和方法实现的安装、卸载操作。

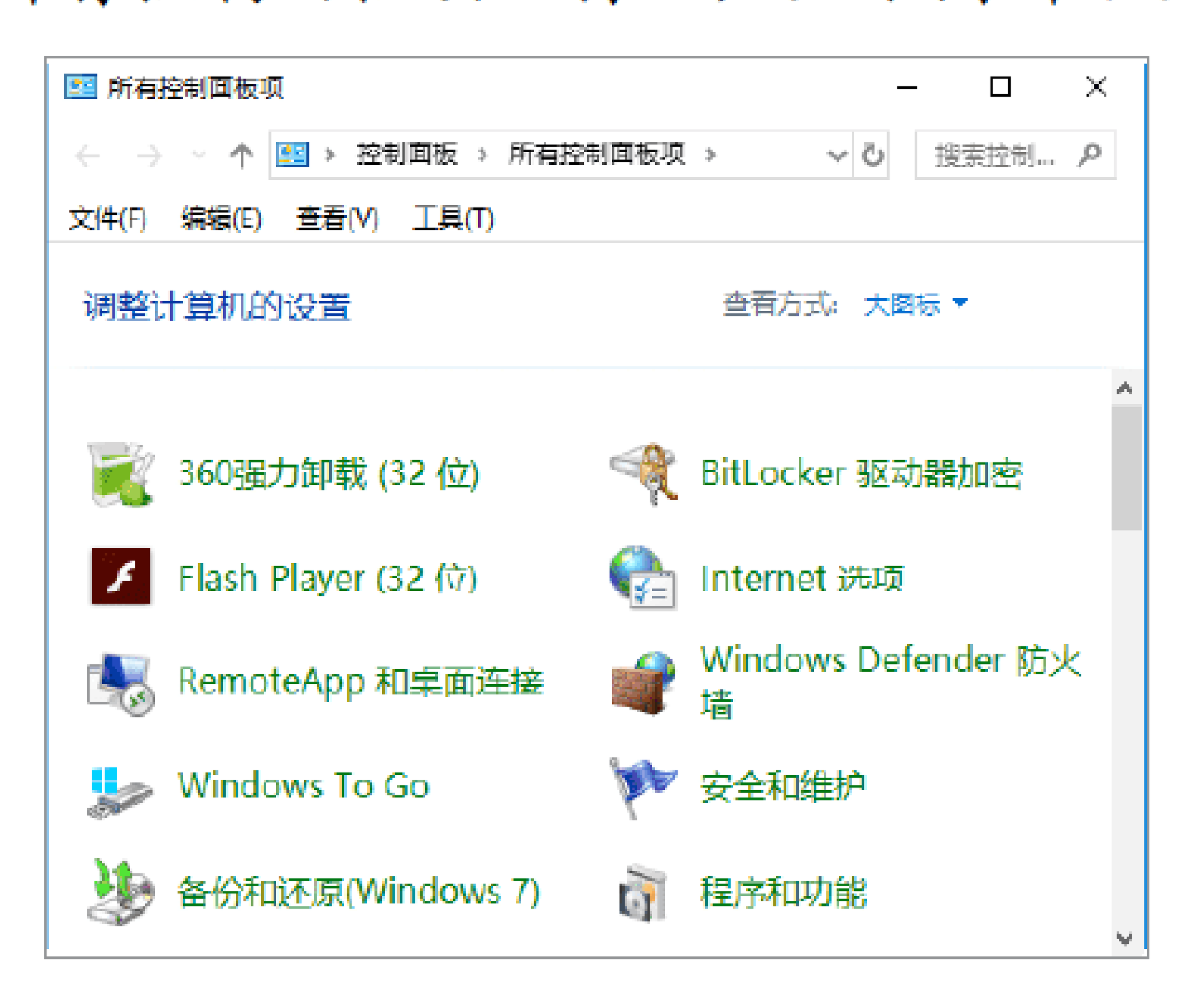
13.6 小试身手



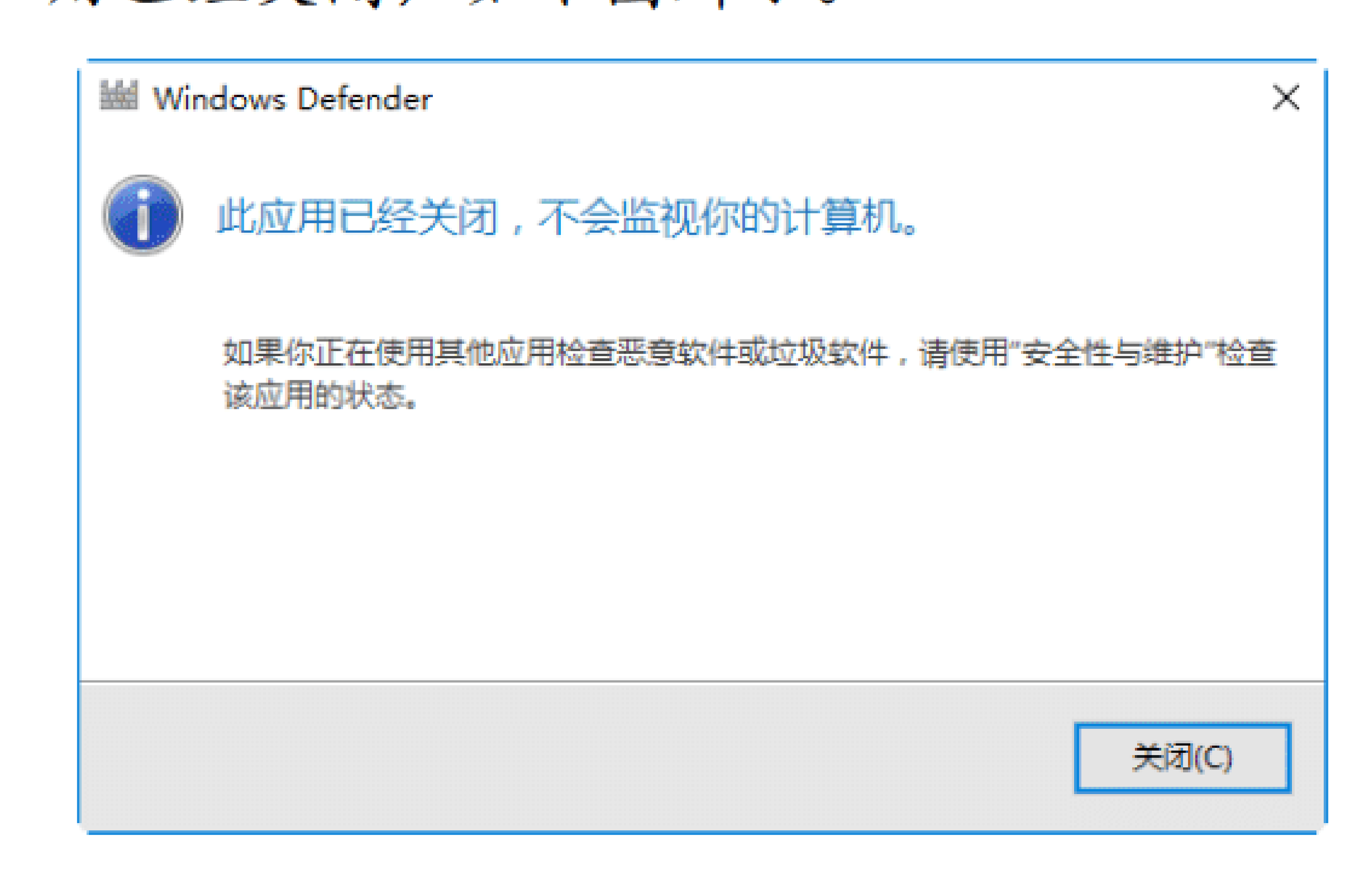
练习1：使用Windows Defender

Windows Defender是Windows 10的一项功能，主要用于帮助用户抵御间谍软件和其他潜在的有害软件的攻击，但在系统默认情况下，该功能是不开启的。下面介绍如何开启Windows Defender功能。具体操作步骤如下。

Step 01 单击“开始”按钮，从弹出的快捷菜单中选择“控制面板”选项，即可打开“所有控制面板项”窗口，如下图所示。



Step 02 单击Windows Defender超链接，即可打开Windows Defender窗口，提示用户此应用已经关闭，如下图所示。



Step 03 在“控制面板”窗口中单击“安全性与维护”超链接，打开“安全性与维护”窗口，如下图所示。



Step 04 单击“间谍软件和垃圾软件防护”后面的“立即启用”按钮，弹出如下图所示对话框。



Step 05 单击“是，我信任这个发布者，希望运行此应用”超链接，即可启用Windows Defender服务，如下图所示。

练习2：管理鼠标的右键菜单

计算机长期使用的过程中，鼠标的右键菜单会越来越长，占了大半个屏幕，看起来绝对不美观、不简洁。这是由于安装软件时附带的添加右键菜单功能而造成的，那么怎么管理右键菜单呢？使用360安全卫士的右键管理功能可以轻松管理鼠标的右键菜单。具体的操作步骤如下。

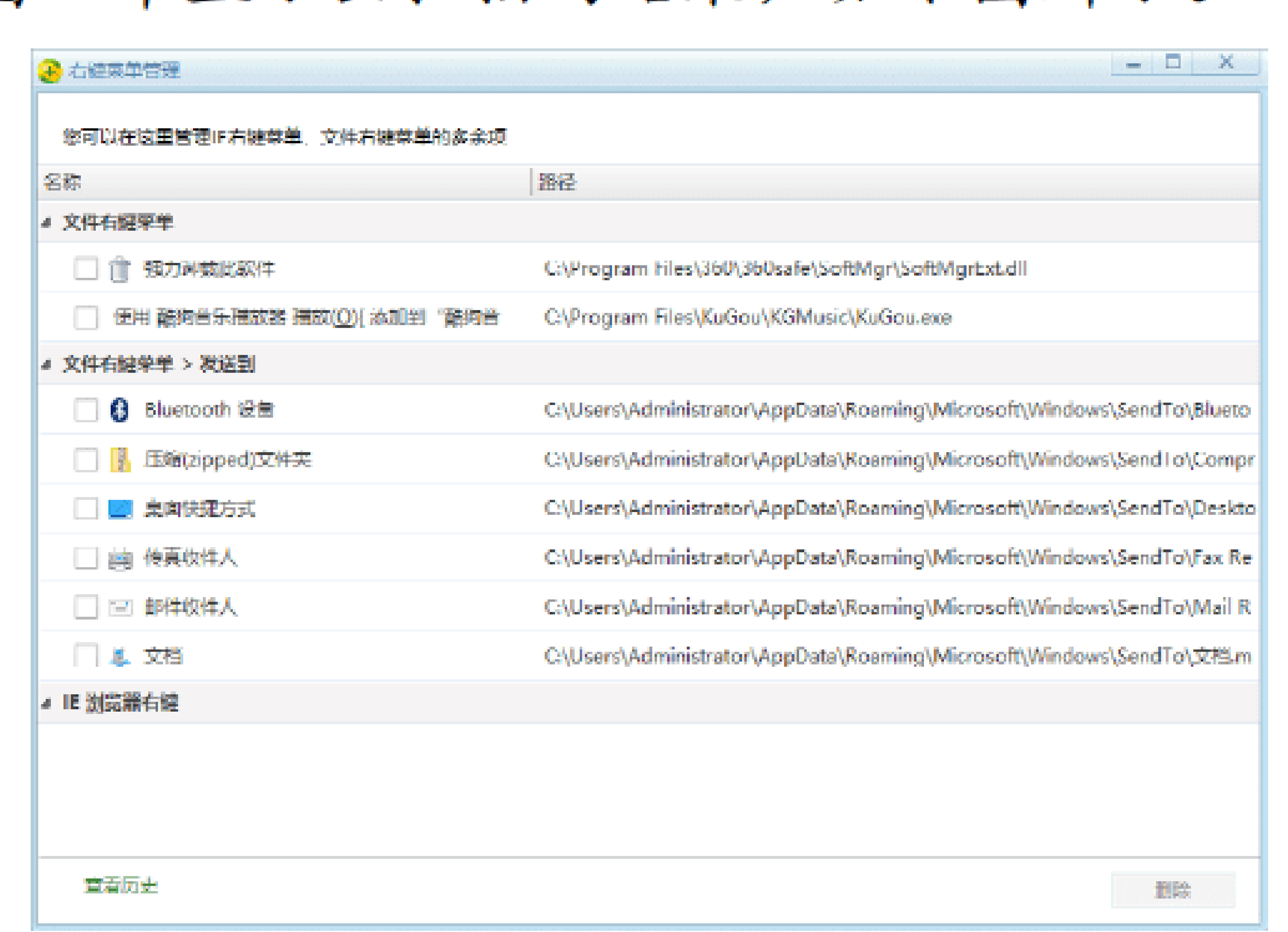
Step 01 在360安全卫士的“全部工具”操作界面中单击“右键管理”图标，如下图所示。



Step 02 打开“右键菜单管理”窗口，如下图所示。

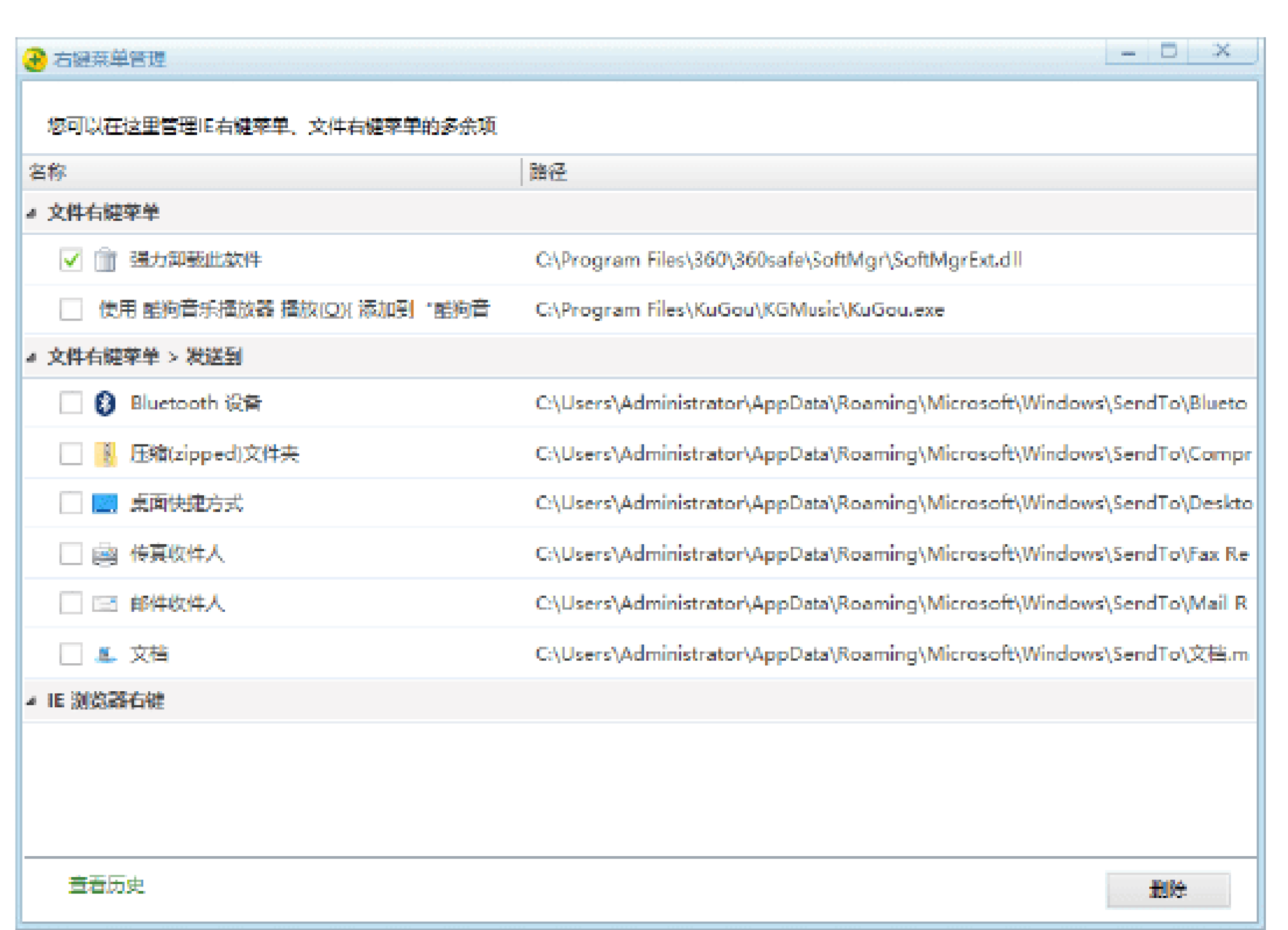


Step 03 单击“开始扫描”按钮，开始扫描右键菜单，扫描完毕后，在“右键菜单管理”窗口中显示出扫描的结果，如下图所示。

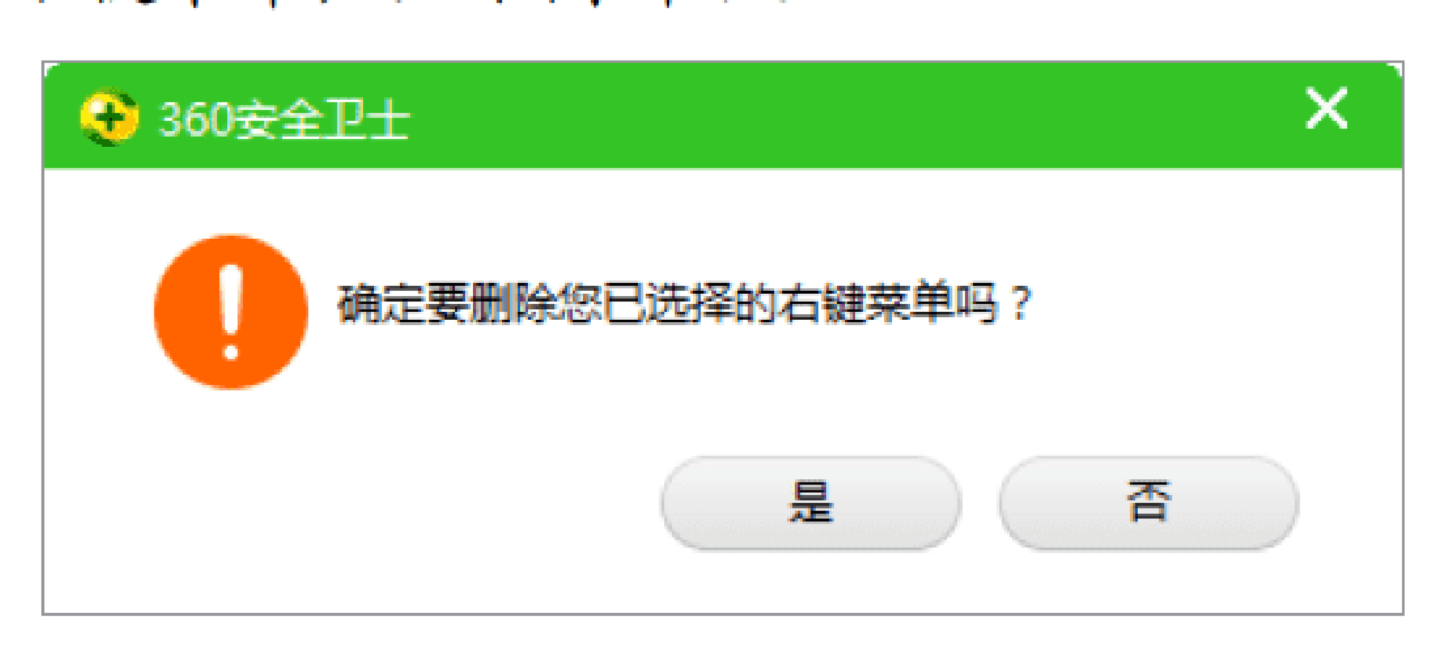


Step 04 勾选需要删除的右键菜单前面的复选框，如下图所示。

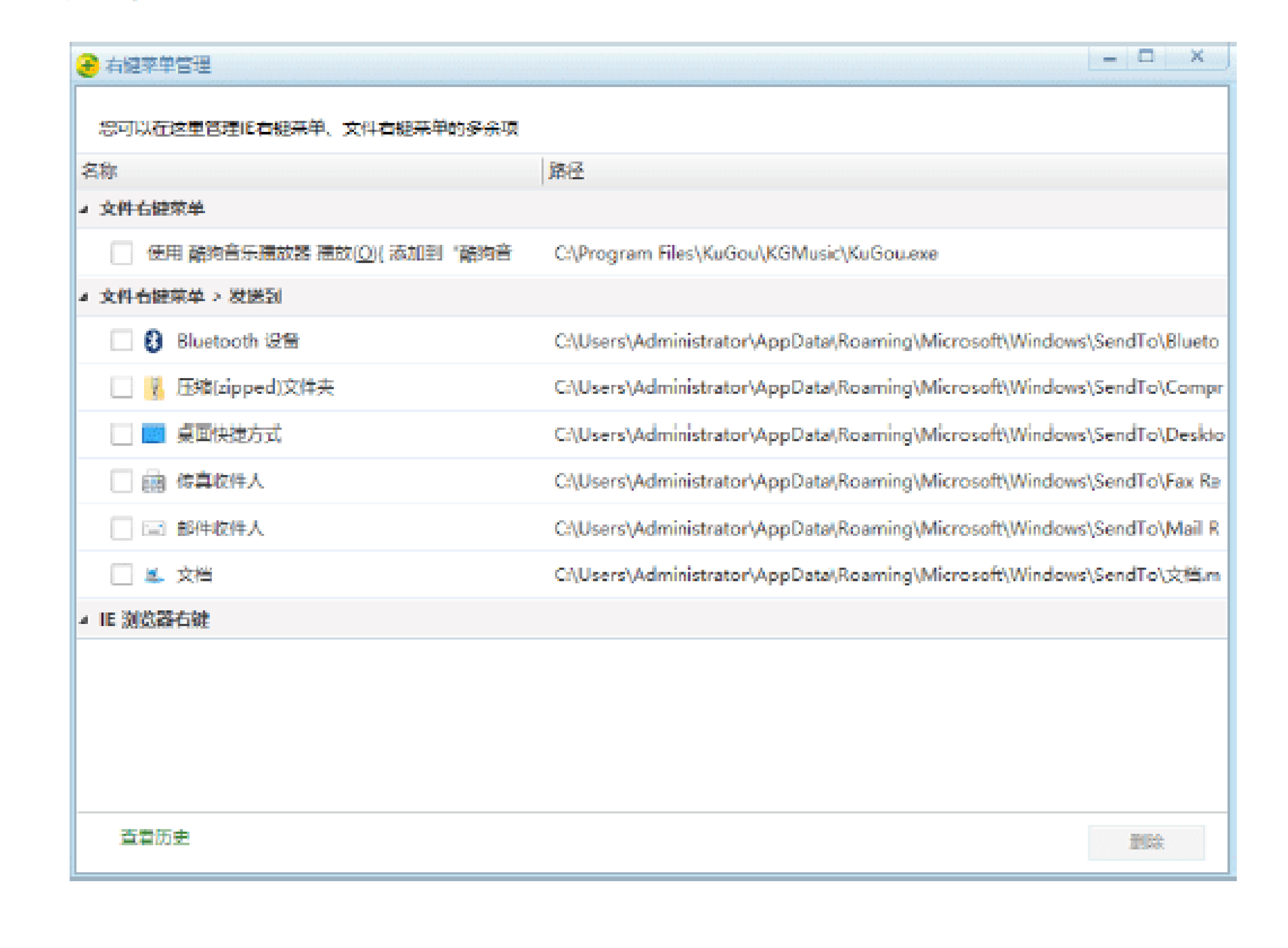




Step 05 单击“删除”按钮，打开信息提示框，提示用户是否确定要删除已经选择的右键菜单，如下图所示。



Step 06 单击“是”按钮，即可将选中的右键菜单删除，如下图所示。



第14章　计算机安全的终极防护

黑客攻击无孔不入，一个小小的漏洞就很有可能使整个系统瘫痪，这时用户就不得不重装系统，但是如果系统进行了备份，那么就可以直接将其还原，以节省时间。本章介绍个人计算机安全的终极防护，主要内容包括重装、备份、还原与重置操作系统等。

14.1　重装计算机操作系统

在安装有一个操作系统的计算机中，用户可以利用安装光盘重装系统，而无须考虑多系统的版本问题，只需将系统安装盘插入光驱，并设置从光驱启动，然后格式化系统盘后，就可以按照安装单操作系统一样重装单系统。

14.1.1　什么情况下重装系统

具体来讲，当系统出现以下3种情况之一，就必须考虑重装系统。

1. 系统运行变慢

系统运行变慢的原因有很多，如垃圾文件分布于整个硬盘而又不便于集中清理和自动清理，或者是计算机感染了病毒或其他恶意程序而无法被杀毒软件清理等，这就需要对磁盘进行格式化处理并重装系统了。

2. 系统频繁出错

众所周知，操作系统是由很多代码组成的，在操作过程中可能因为误删除某个文件或者是被恶意代码改写等原因，致使系统出现错误，此时，如果该故障不便于准确定位或轻易解决，就需要考虑重装系统了。

3. 系统无法启动

导致系统无法启动的原因有多种，如DOS引导出现错误、目录表被损坏或系统文件ntfs.sys文件丢失等。如果无法查找出系统不能启动的原因或无法修复系统以解决这一问题时，就需要重装系统了。

14.1.2　重装前应注意的事项

在重装系统之前，用户需要做好充分的准备，以避免重装之后造成数据的丢失等严重后果。那么在重装系统之前应该注意哪些事项呢？

1. 备份数据

在因系统崩溃或出现故障而准备重装系统之前，首先应该想到的是备份好自己的数据。这时，一定要静下心来，仔细罗列一下硬盘中需要备份的资料，把它们一项一项地写在一张纸上，然后逐一对照进行备份。如果硬盘不能启动，这时需要考虑用其他启动盘启动系统，然后复制自己的数据，或将硬盘挂接到其他计算机上进行备份。但是，最好的办法是在平时就养成每天备份重要数据的习惯，这样就可以有效避免硬盘数据不能恢复造成的损失。

2. 格式化磁盘

重装系统时，格式化磁盘是解决系统问题最有效的办法，尤其是在系统感染病毒后，最好不要只格式化C盘，如果有条件将硬盘中的数据都备份或转移，尽量备份后将整个硬盘都格式化，以保证新系统的安全。

3. 牢记安装序列号

安装序列号相当于一个人的身份证号，标识着安装程序的身份。如果不小心丢掉自己的安装序列号，那么在重装系统时，如果

采用的是全新安装，安装过程将无法进行下去。正规的安装光盘的序列号会标注在软件说明书或光盘封套的某个位置上。但是，如果用的是某些软件合集光盘中提供的测试版系统，那么，这些序列号可能存在于安装目录中的某个说明文本中，如SN.txt等文件。因此，在重装系统之前，首先将序列号找出并记录下来，以备稍后使用。

实战1：重装Windows 10操作系统

Windows 10作为新一代操作系统，备受关注，下面将介绍Windows 10操作系统的重装，具体步骤如下。

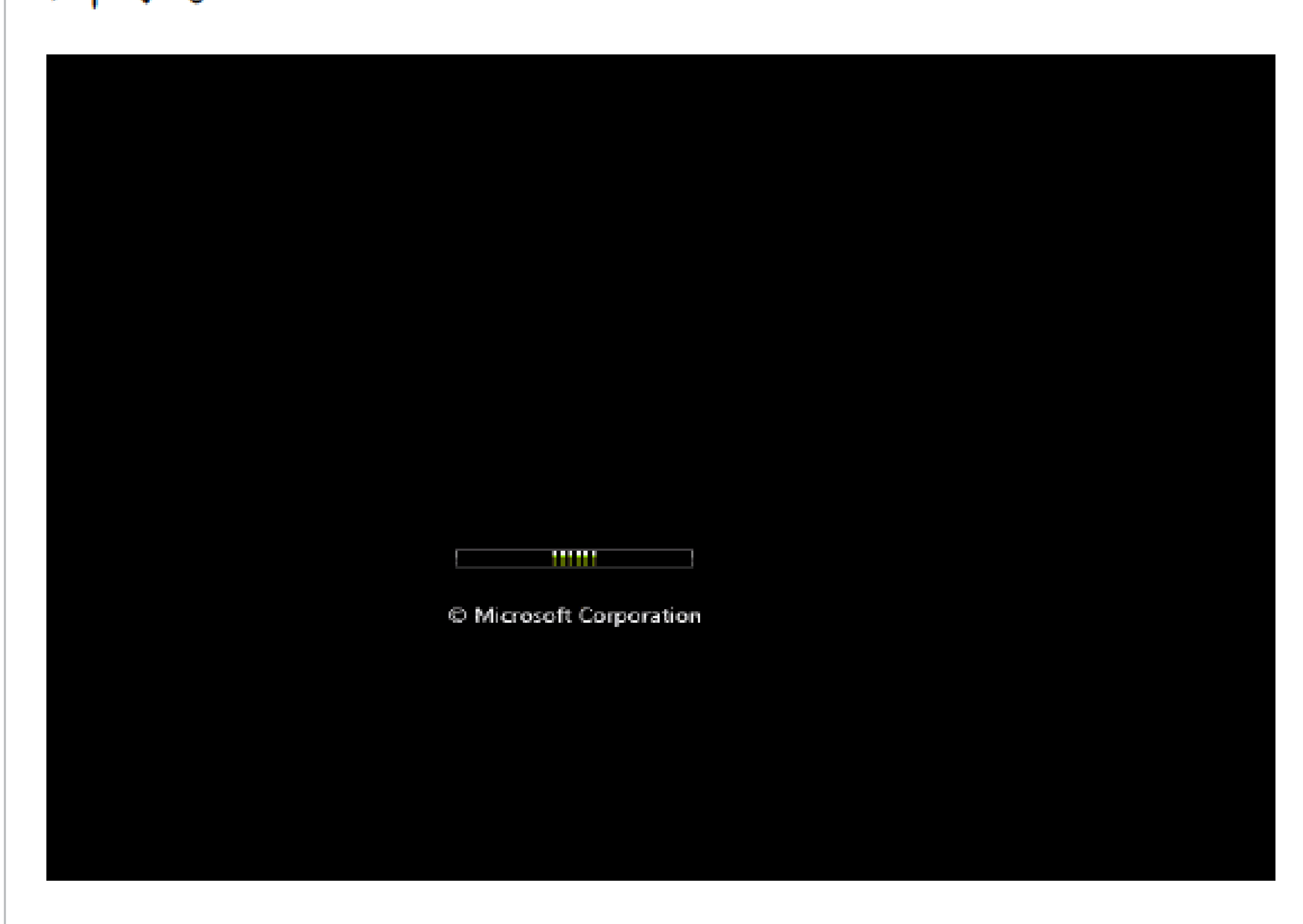
Step 01 将Windows 10操作系统的安装光盘放入光驱中，重新启动计算机，这时会进入Windows 10操作系统安装程序的运行窗口，提示用户安装程序正在加载文件，如下图所示。



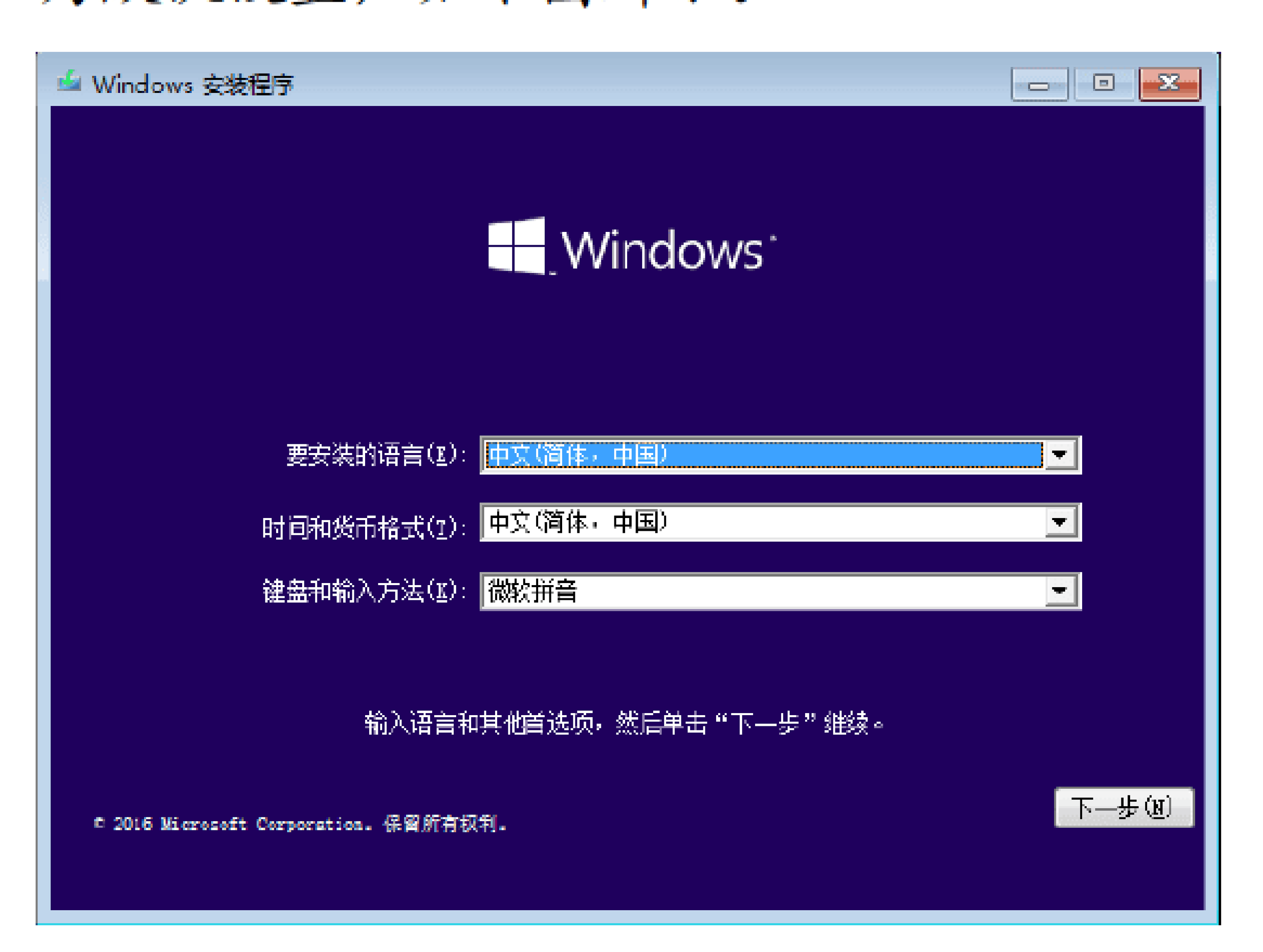
Step 02 当文件加载完成后，进入程序，启动Windows界面，如下图所示。



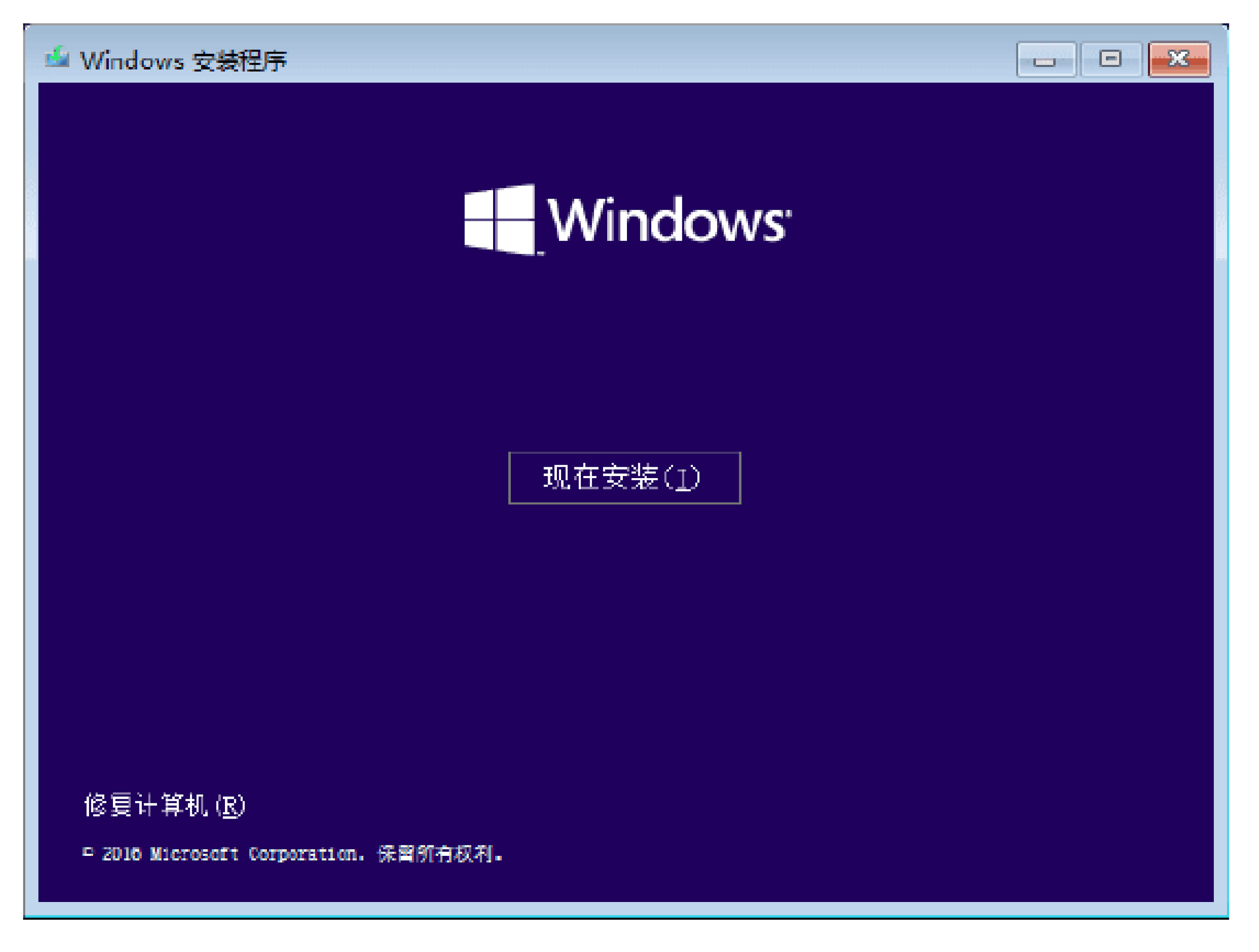
Step 03 进入程序运行界面，开始运行程序，并且显示程序的运行速度，如下图所示。



Step 04 运行程序完成，就会弹出安装Windows对话框，根据需求进行设置，一般为默认设置，如下图所示。



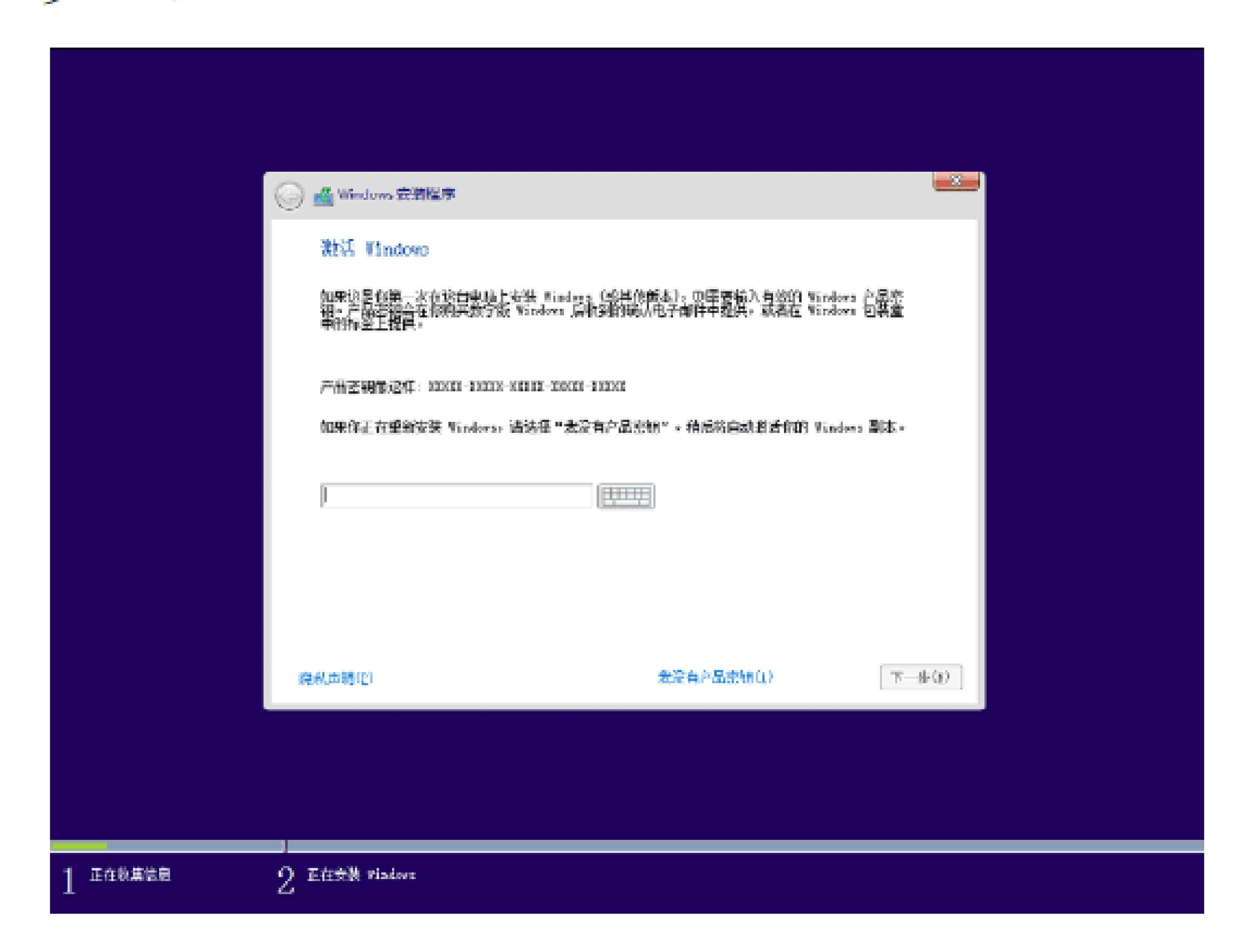
Step 05 设置完成后，单击“下一步”按钮，进入安装确认操作页面，如下图所示。



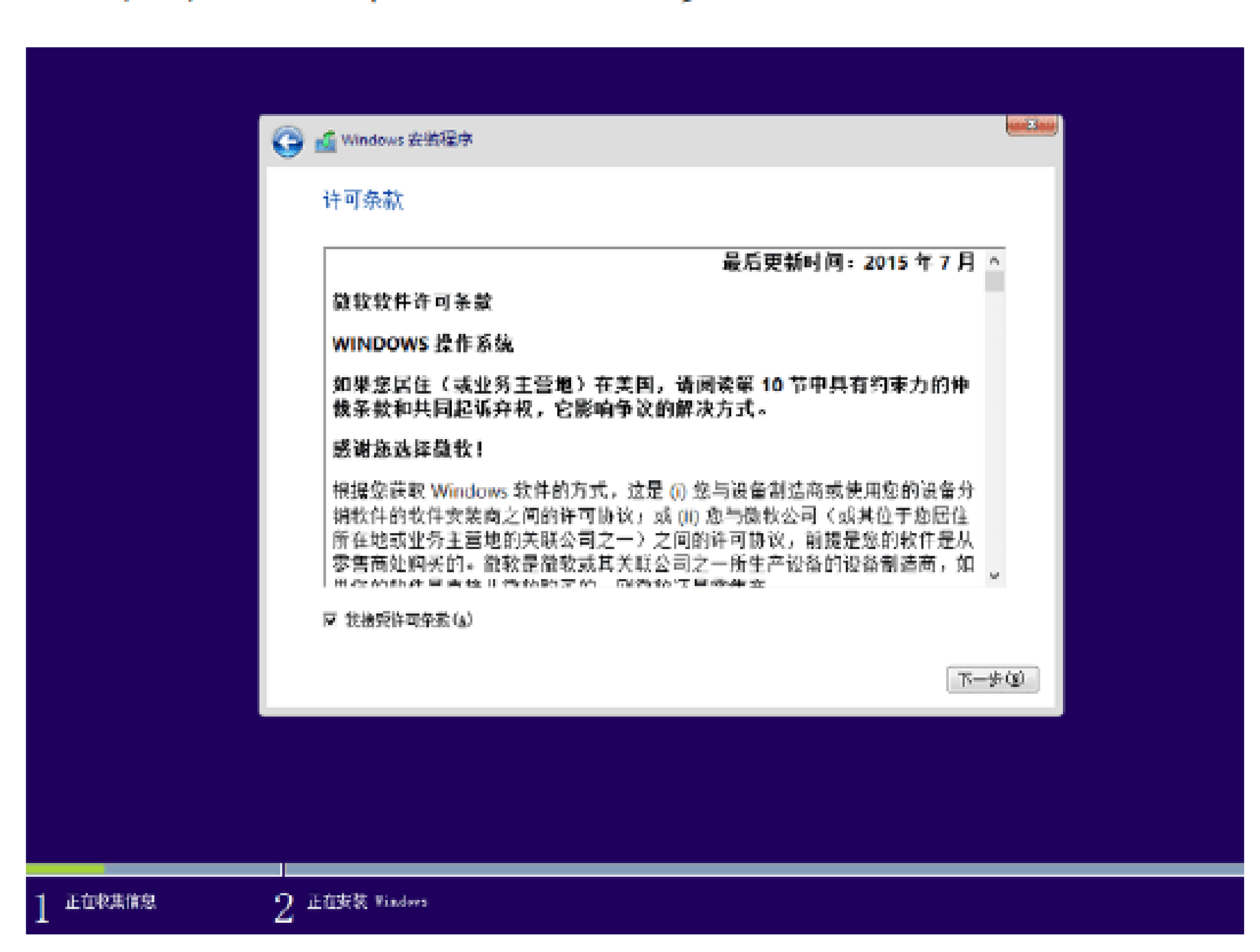
Step 06 单击“现在安装”按钮，进入“安装程序正在启动”页面，如下图所示。



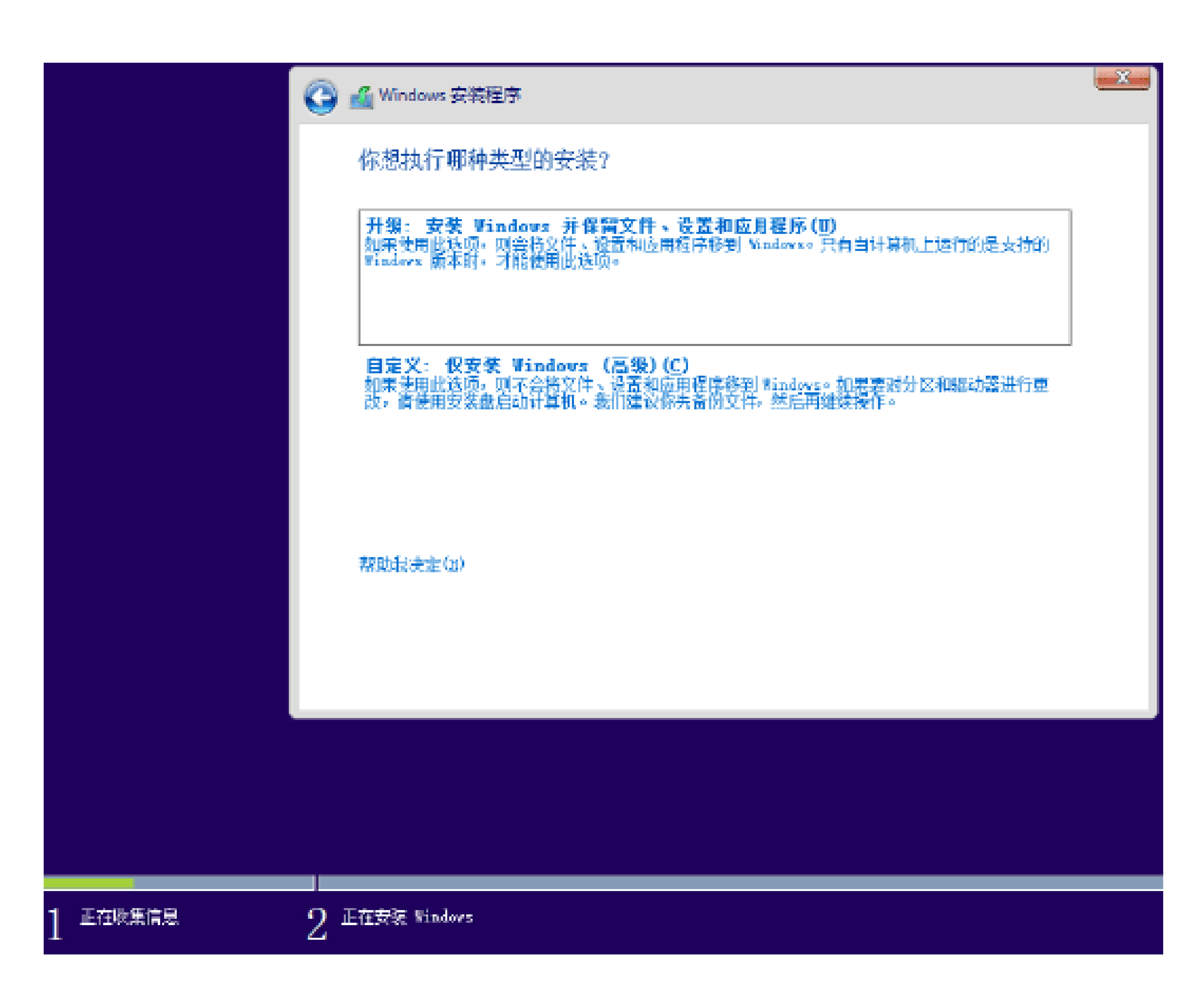
Step 07 稍后进入“激活Windows”页面，如下图所示，需要在此页面输入Windows 10操作系统的产品密钥，然后单击“下一步”按钮。



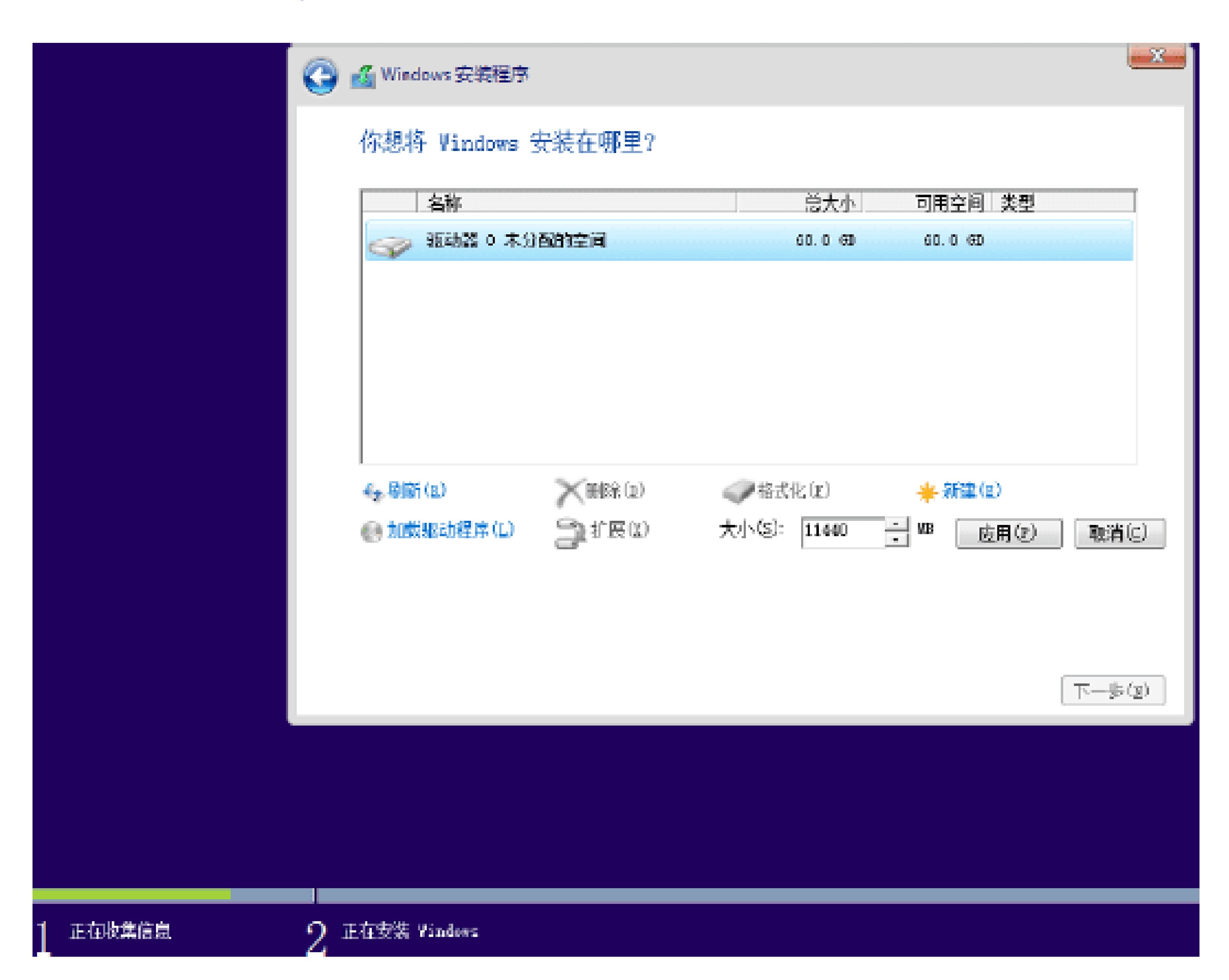
Step 08 接下来进入“许可条款”页面，在此页面勾选“我接受许可条款”复选框，如下图所示，单击“下一步”按钮。



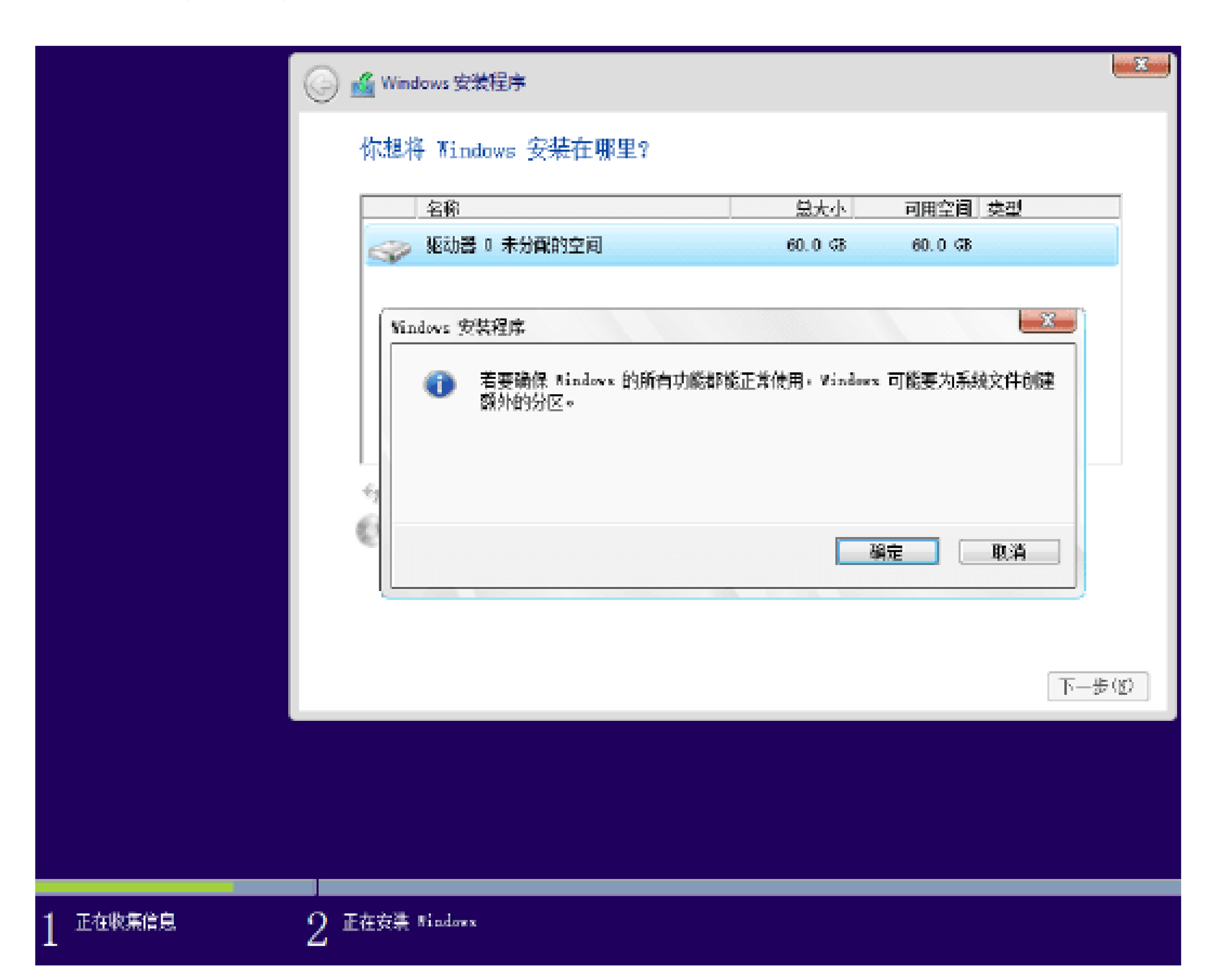
Step 09 进入“你想执行哪种类型的安装？”页面，这里选择“自定义：仅安装Windows（高级）”选项，如下图所示。如果需要升级，则单击“升级：安装Windows并保留文件、设置和应用程序”选项。



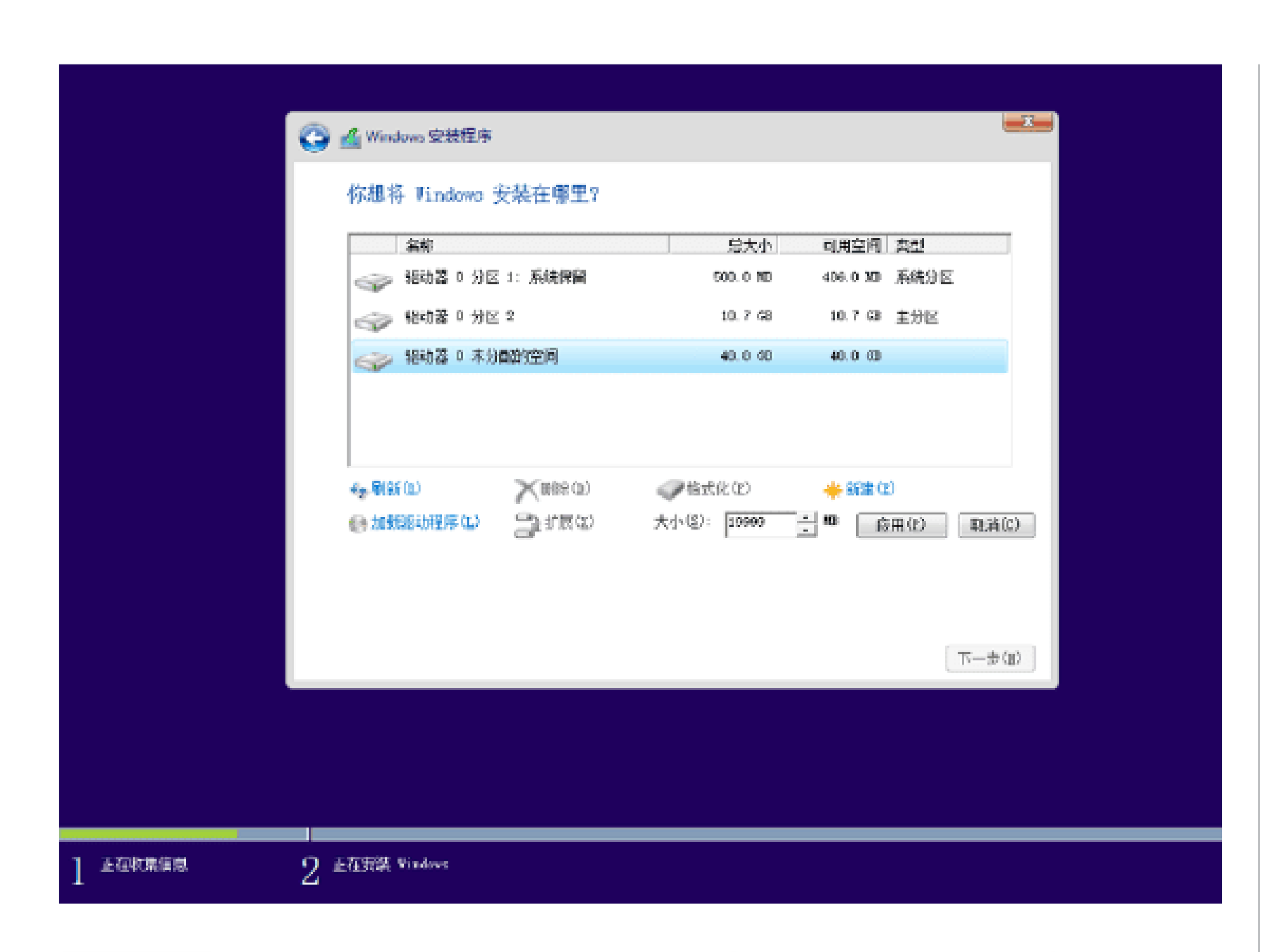
Step 10 进入“你想将Windows安装在哪里？”界面，如下图所示，单击“新建”链接，开始创建硬盘分区，填写硬盘分区的大小，单击“应用”按钮。



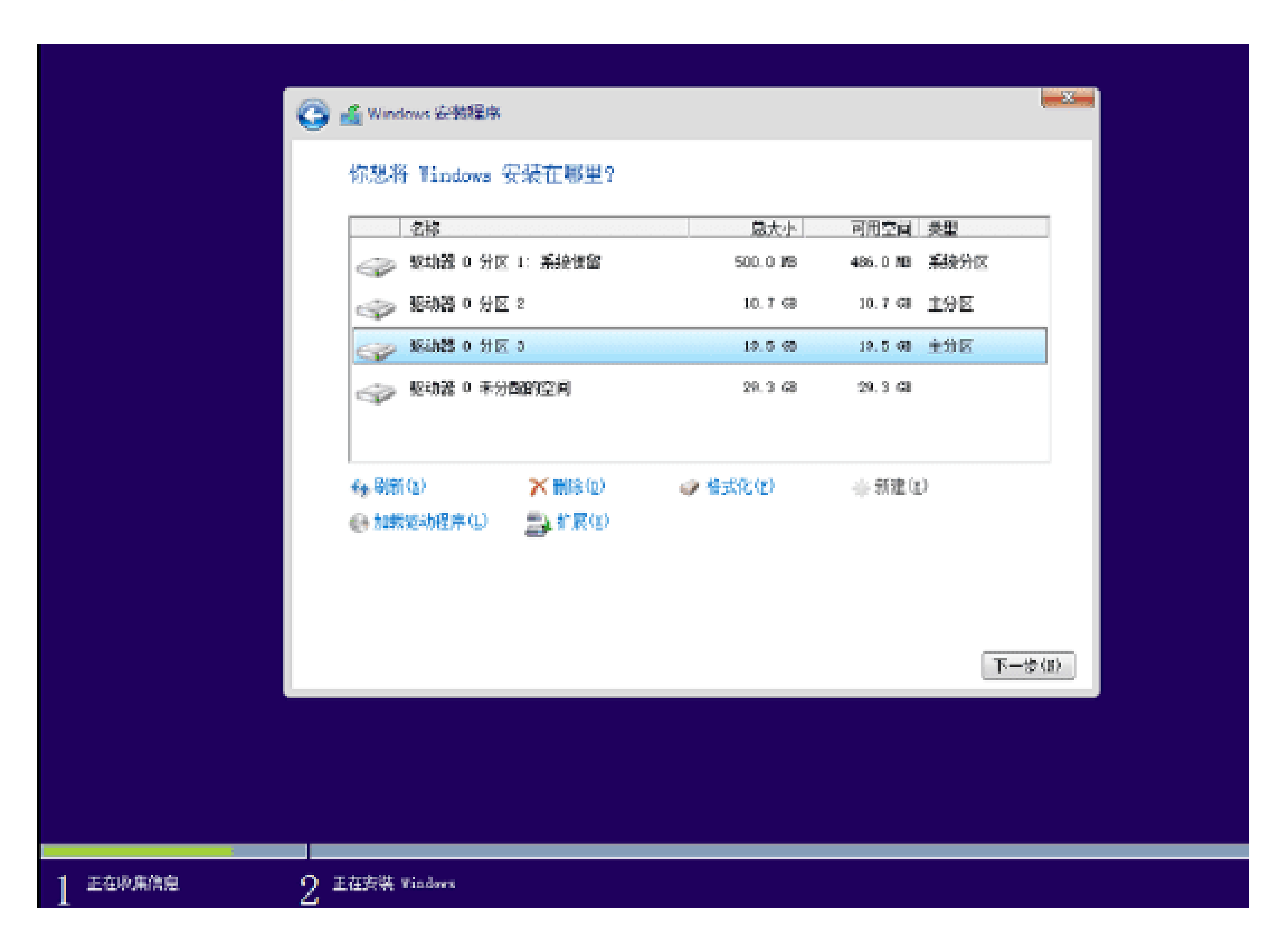
Step 11 弹出确认提示框，如下图所示，单击“确定”按钮。



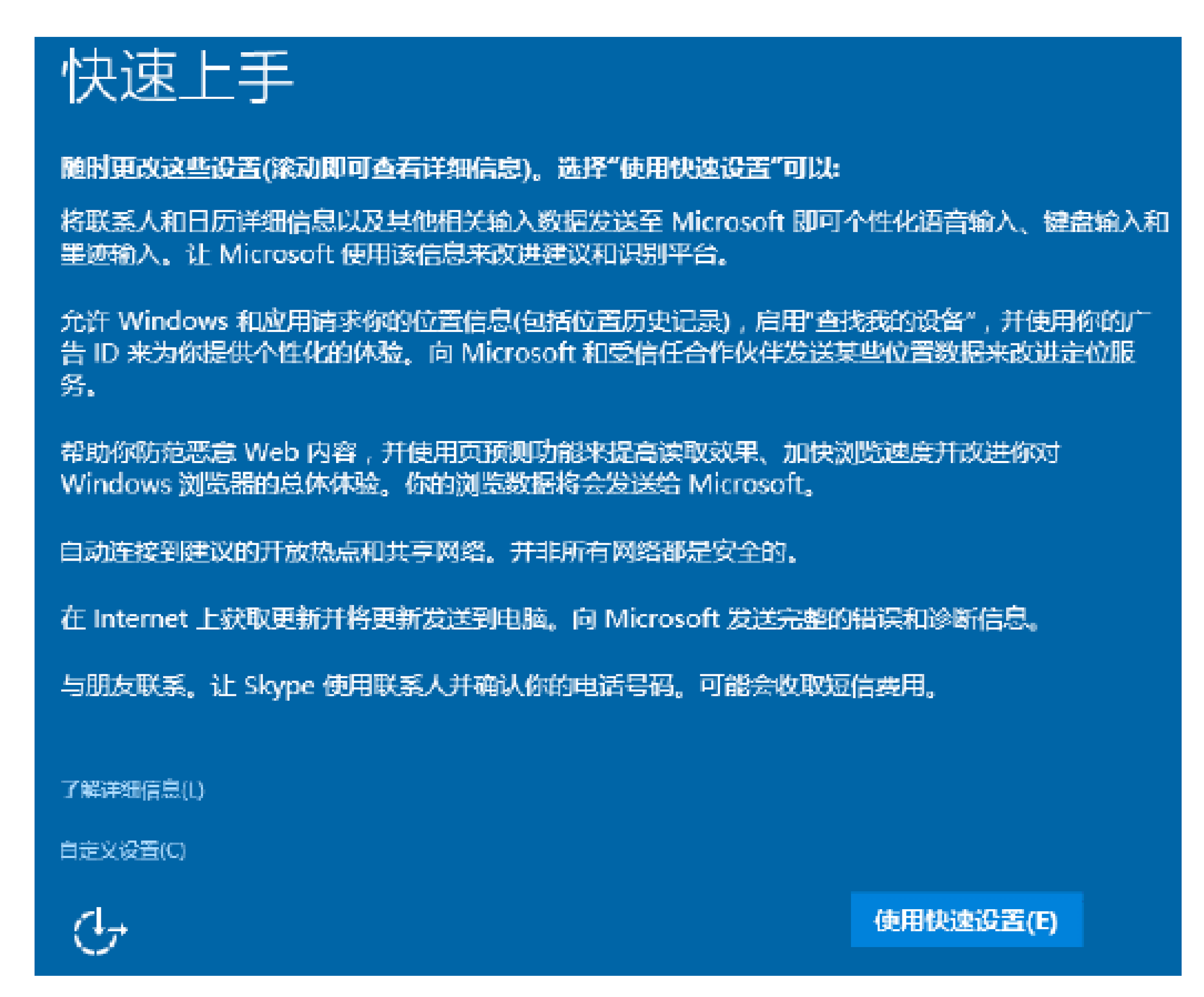
Step 12 第一个分区完成，如果还想继续为硬盘分区，单击“新建”链接就可以，如下图所示。



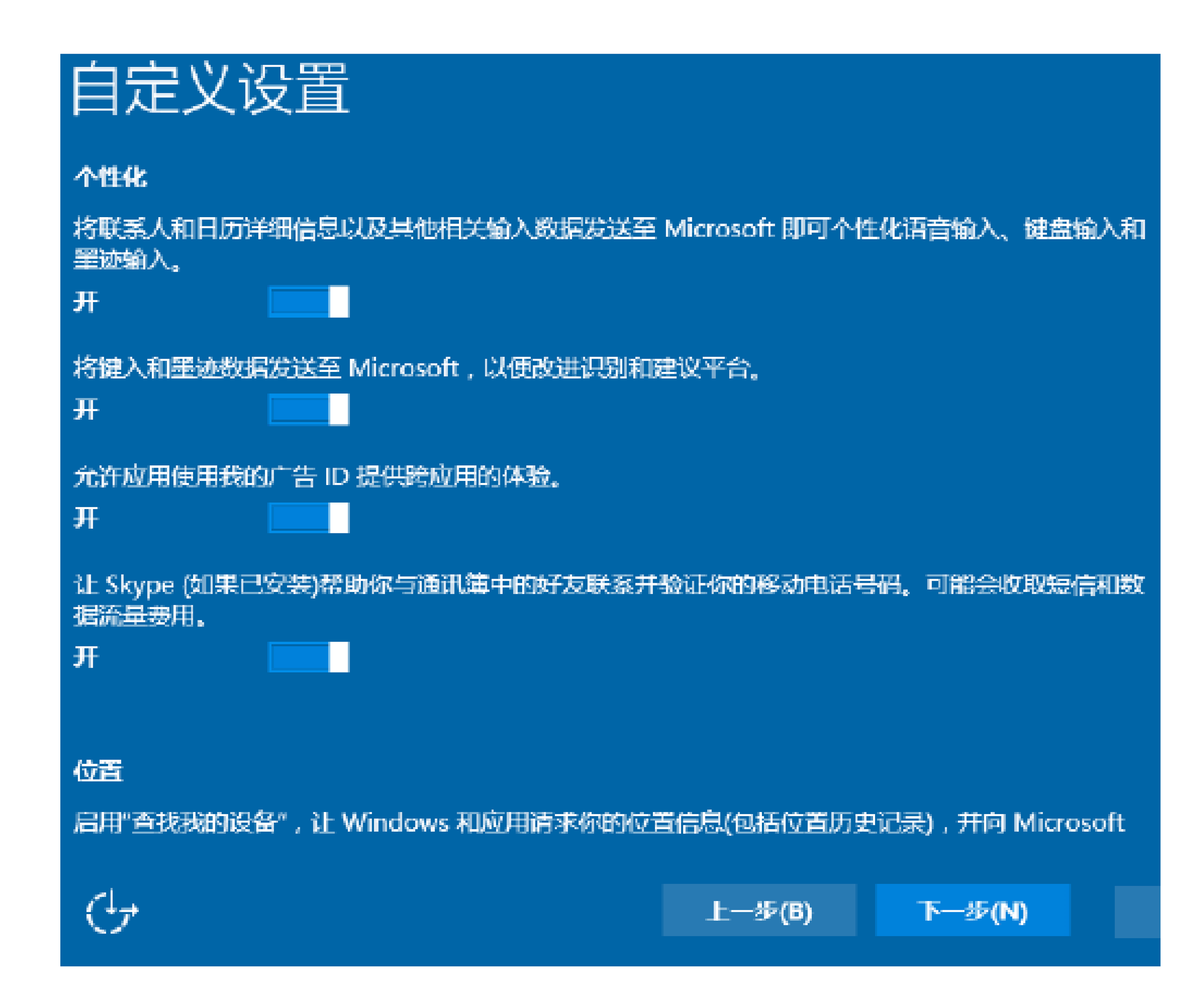
Step 13 硬盘分区完成，单击“下一步”按钮，如下图所示。



Step 14 驱动准备完成以后，接下来进入系统的设置引导界面，对Windows 10进行设置，可以直接单击右下角的“使用快速设置”来使用默认设置，也可以单击屏幕左下角的“自定义设置”来逐项设置。在这里直接单击“使用快速设置”按钮，如下图所示。



Step 15 接下来进入“自定义设置”页面，根据需要设置快捷方式，如下图所示。



Step 16 自定义设置完成，单击“下一步”按钮，稍等一会，接下来进入设置账户页面，根据用户的使用选择计算机所有者，如下图所示。在这里选择“我拥有它”选项，单击“下一步”按钮。

谁是这台电脑的所有者？

我的工作单位或学校拥有它

我们会将它设置为归工作单位或学校所有，并且你将能够访问其资源(网络、电子邮件、应用等)。它们将对此电脑拥有完全控制权。

我拥有它

我们将使用 Microsoft 帐户将它设置为归你所有。

下一步

Step 17 进入“个性化设置”页面，拥有Microsoft账户可以进行登录，没有账户的，可以进行创建，这里选择“跳过此步骤”选项，如下图所示。

个性化设置

你的 Microsoft 帐户为你提供了很多权益。登录开始你的个性化体验。了解详细信息

电子邮件或电话号码

密码

忘记密码了

没有帐户? 创建一个!

跳过此步骤

Microsoft 隐私声明

后退　登录



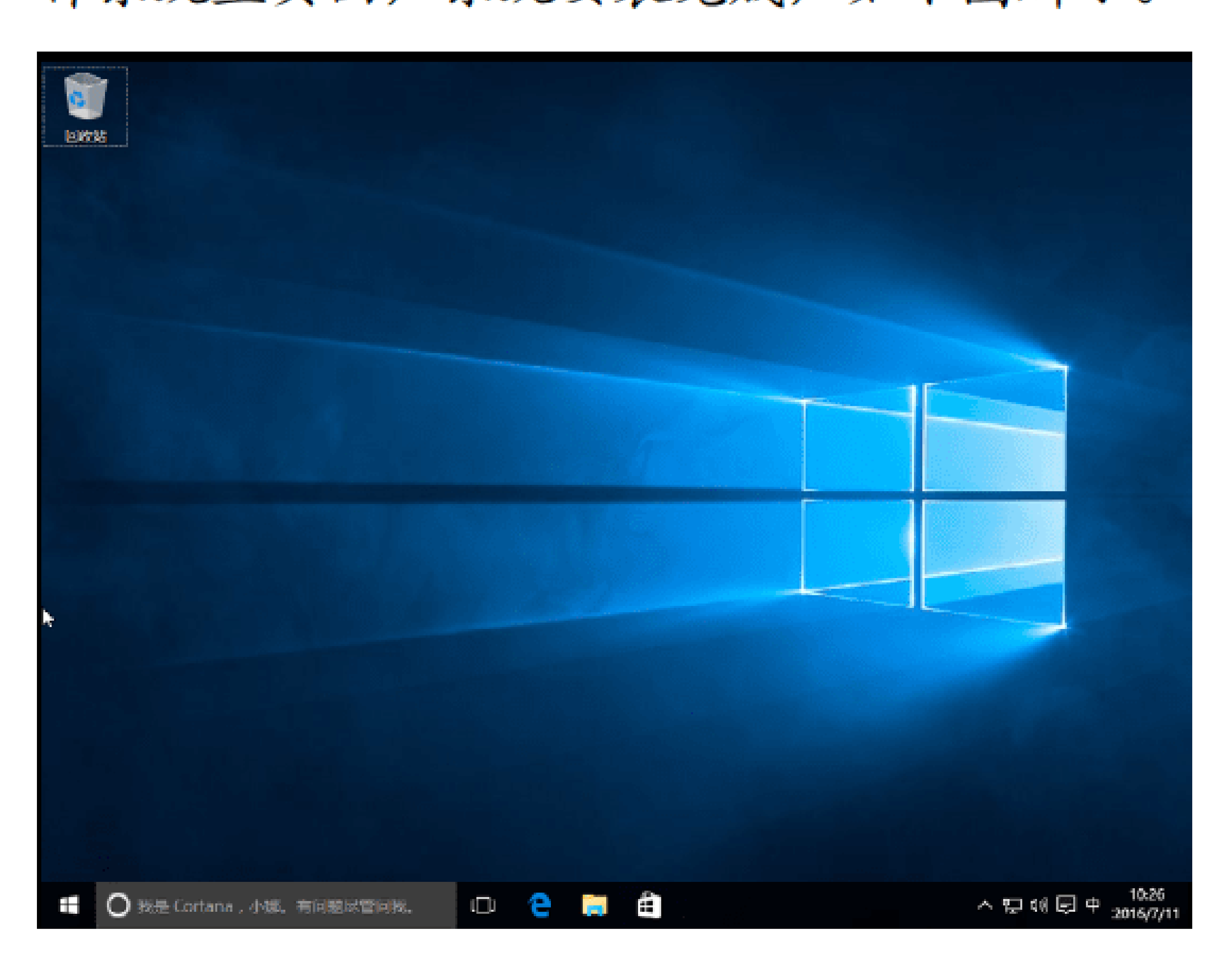
Step 18 进入“为这台计算机创建一个账户”页面，输入用户名、密码和密码提示，如下图所示，单击“下一步”按钮。



Step 19 进入Windows 10操作系统引导页面，如下图所示。



Step 20 跳过系统引导页面，进入Windows 10操作系统主页面，系统安装完成，如下图所示。



14.2 备份计算机操作系统

常见备份系统的方法为使用系统自带的工具备份和Ghost工具备份。

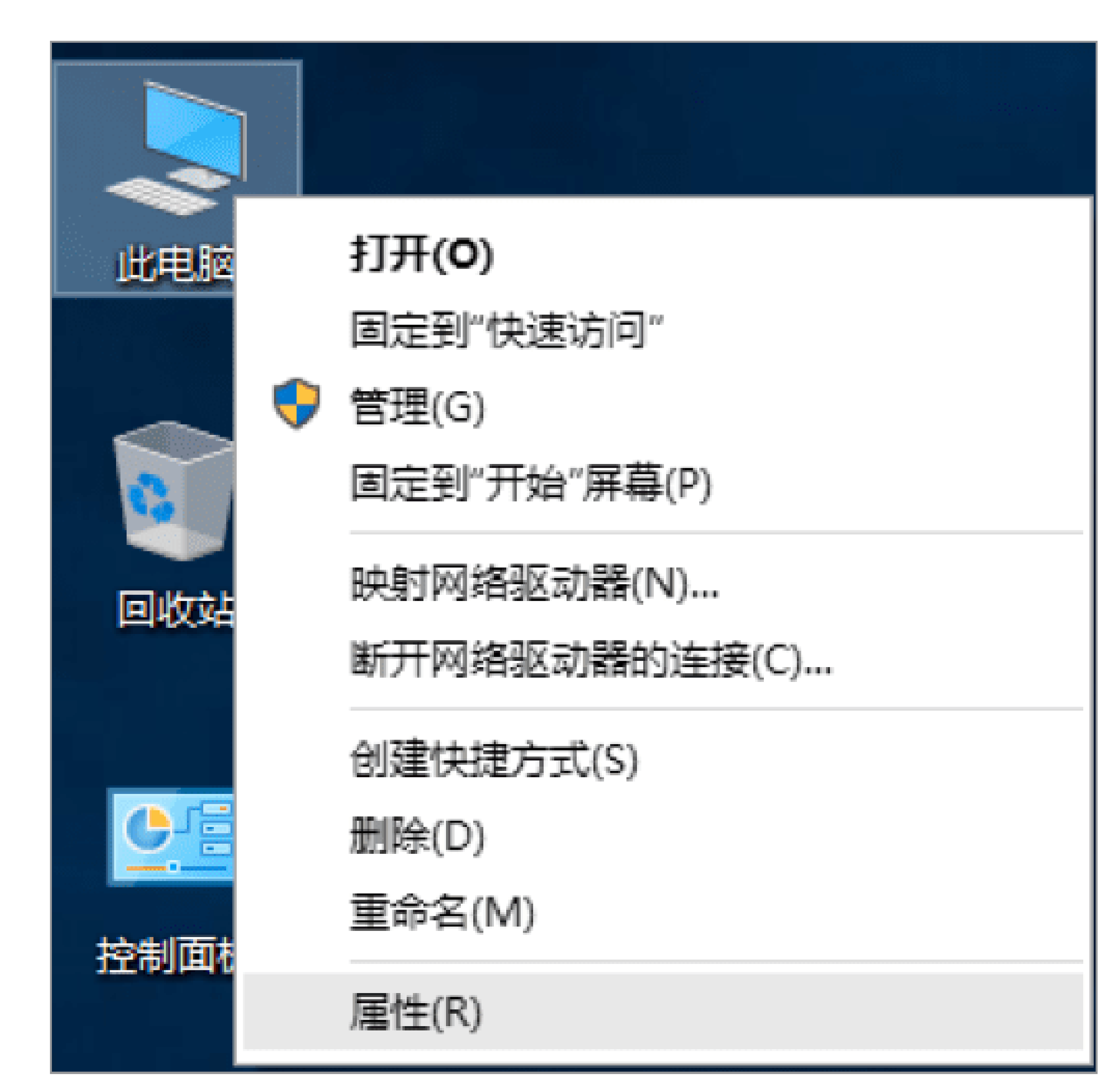
实战2：使用系统工具备份系统

Windows 10操作系统自带的备份还原功能更加强大，为用户提供了高速度、高压缩的一键备份还原功能。

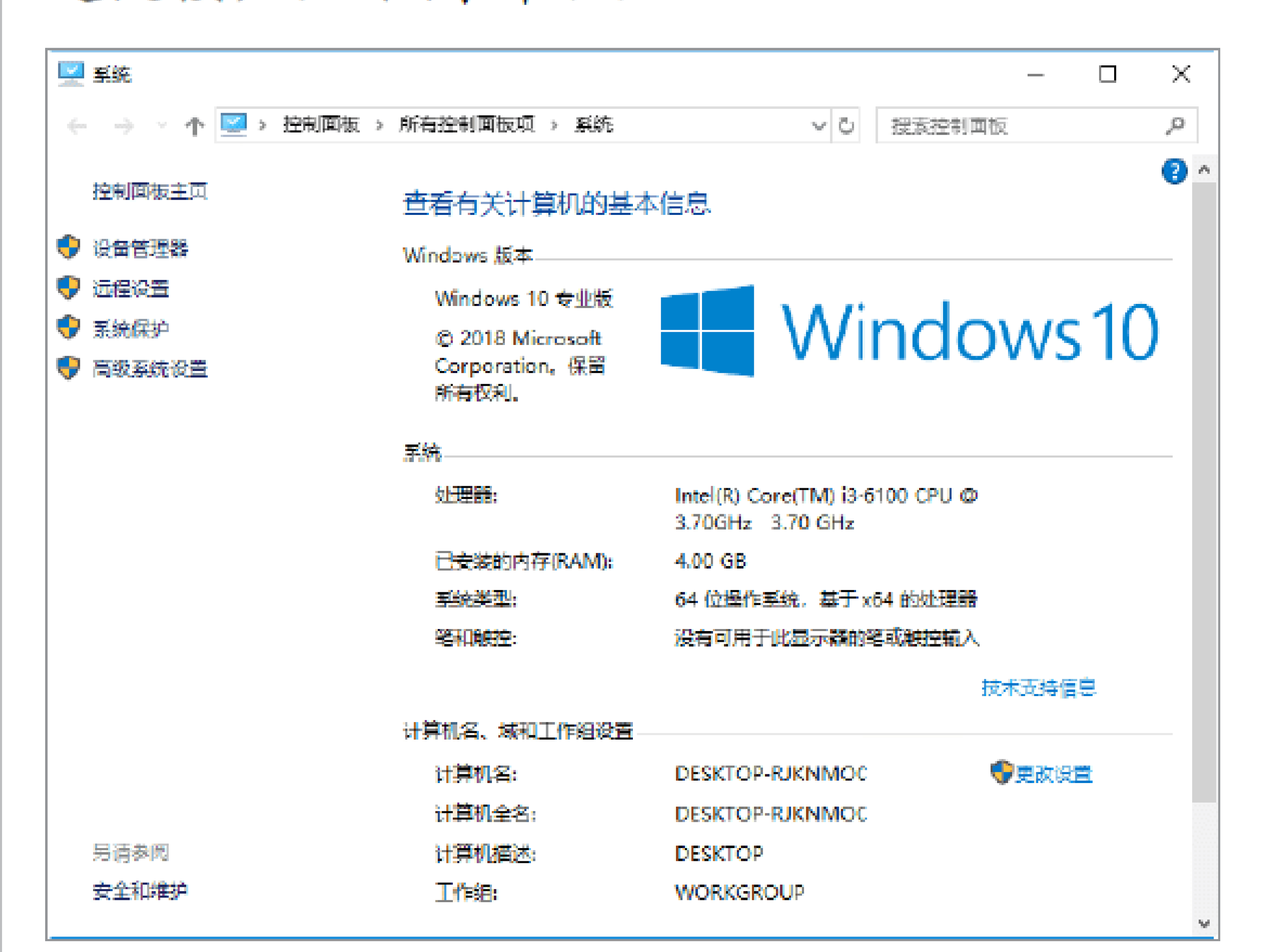
1. 开启系统还原功能

要想使用Windows系统工具备份和还原系统，首先需要开启系统还原功能。具体的操作步骤如下。

Step 01 右键单击计算机桌面上的“此计算机”图标，在打开快捷菜单命令中选择“属性”选项，如下图所示。



Step 02 在打开的窗口中，单击“系统保护”超链接，如下图所示。



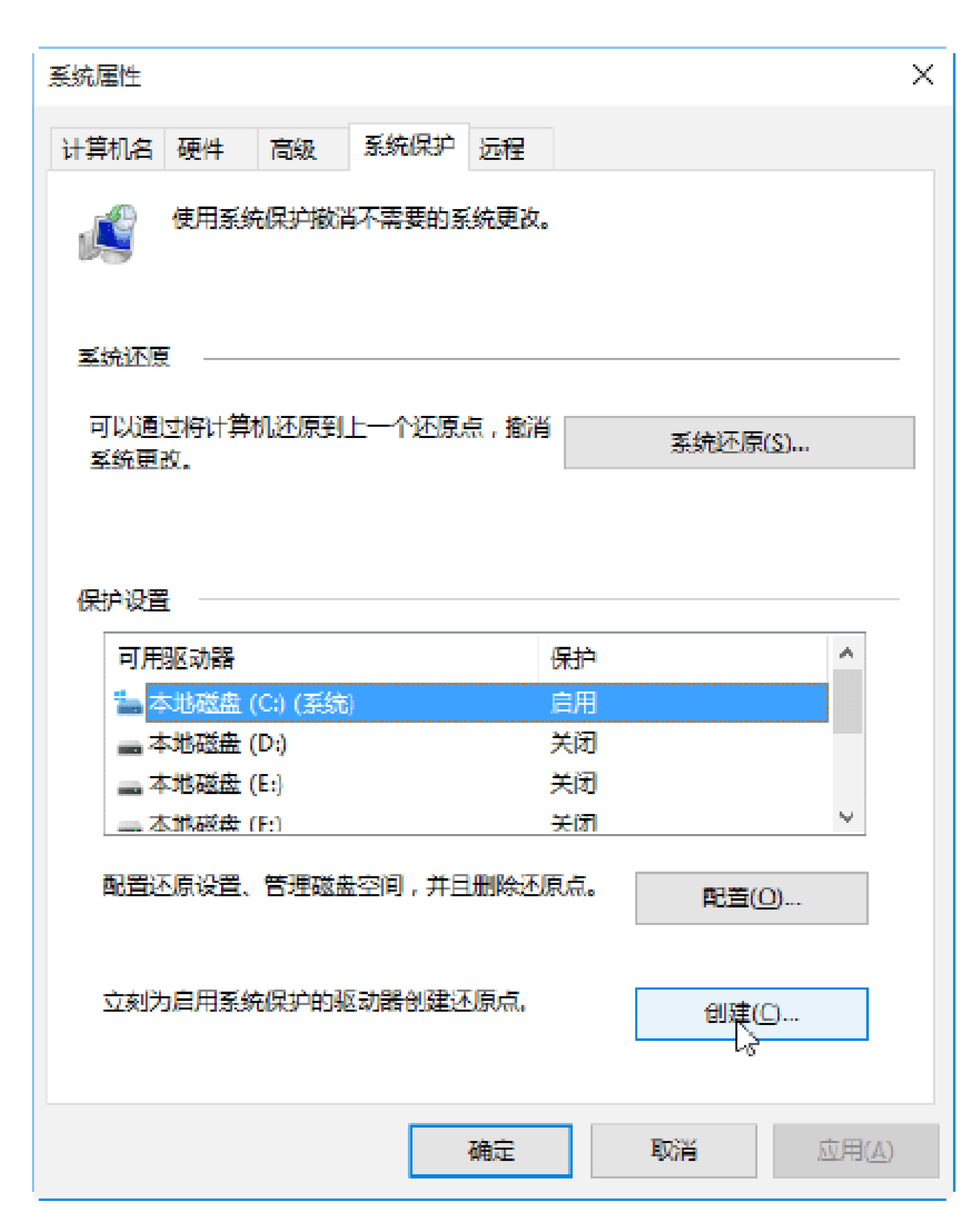
Step 03 弹出“系统属性”对话框，在“保护设置”列表框中选择系统所在的分区，如下图所示，并单击“配置”按钮。

Step 04 弹出“系统保护本地磁盘”对话框，单击选中“启用系统保护”单选按钮，单击鼠标调整“最大使用量”滑块到合适的位置，如下图所示，然后单击“确定”按钮。

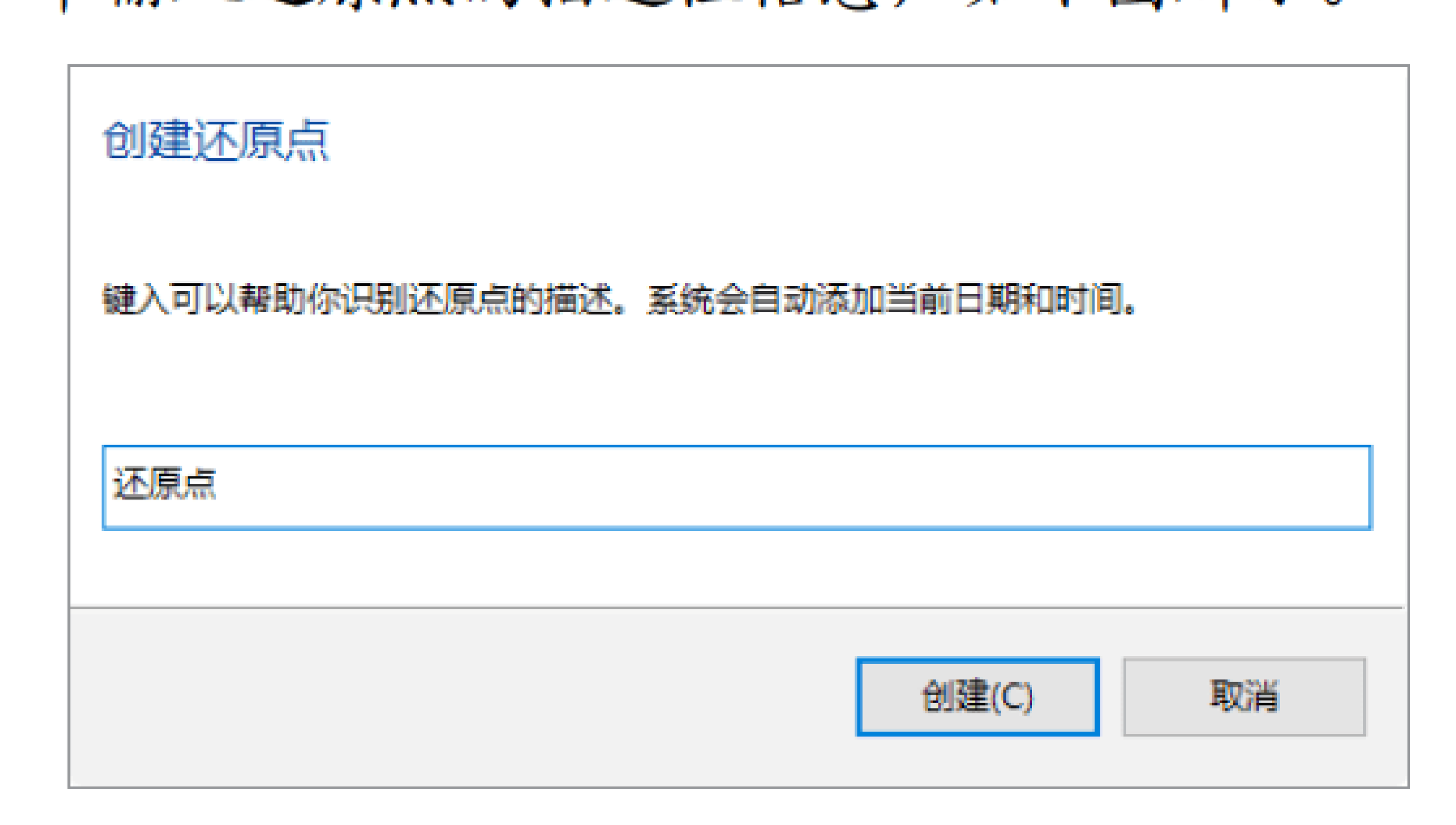
2. 创建系统还原点

用户开启系统还原功能后，默认打开保护系统文件和设置的相关信息，保护系统。用户也可以创建系统还原点，当系统出现问题时，就可以方便地恢复到创建还原点时的状态。

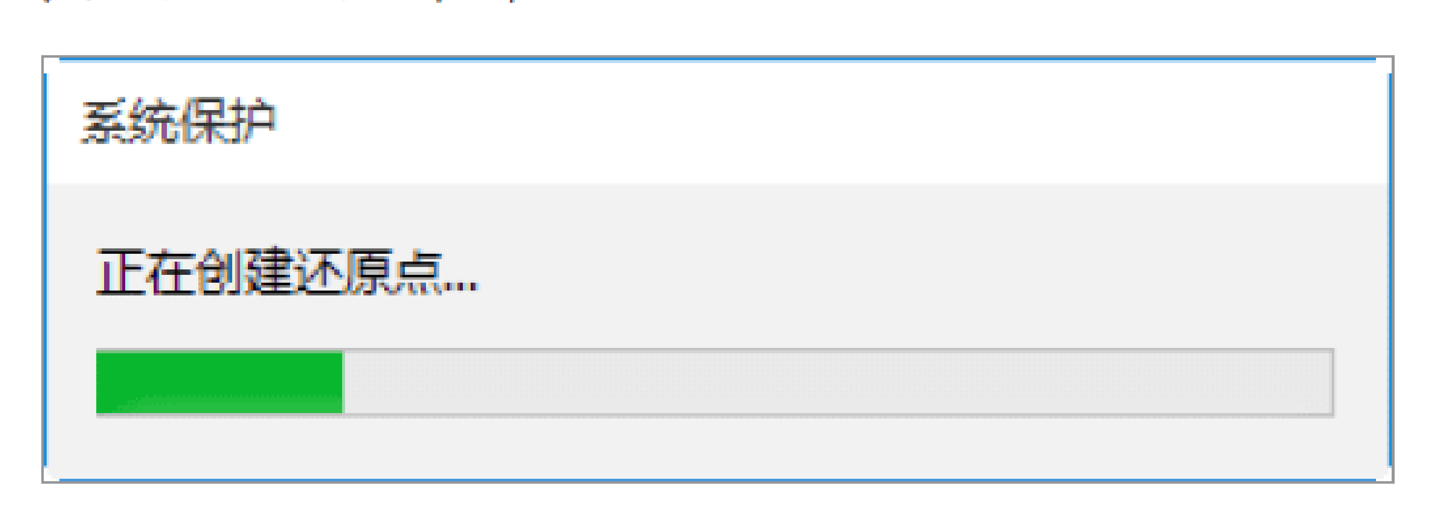
Step 01 在打开的“系统属性”对话框中，选择“系统保护”选项卡，然后选择系统所在的分区，如下图所示，单击“创建”按钮。



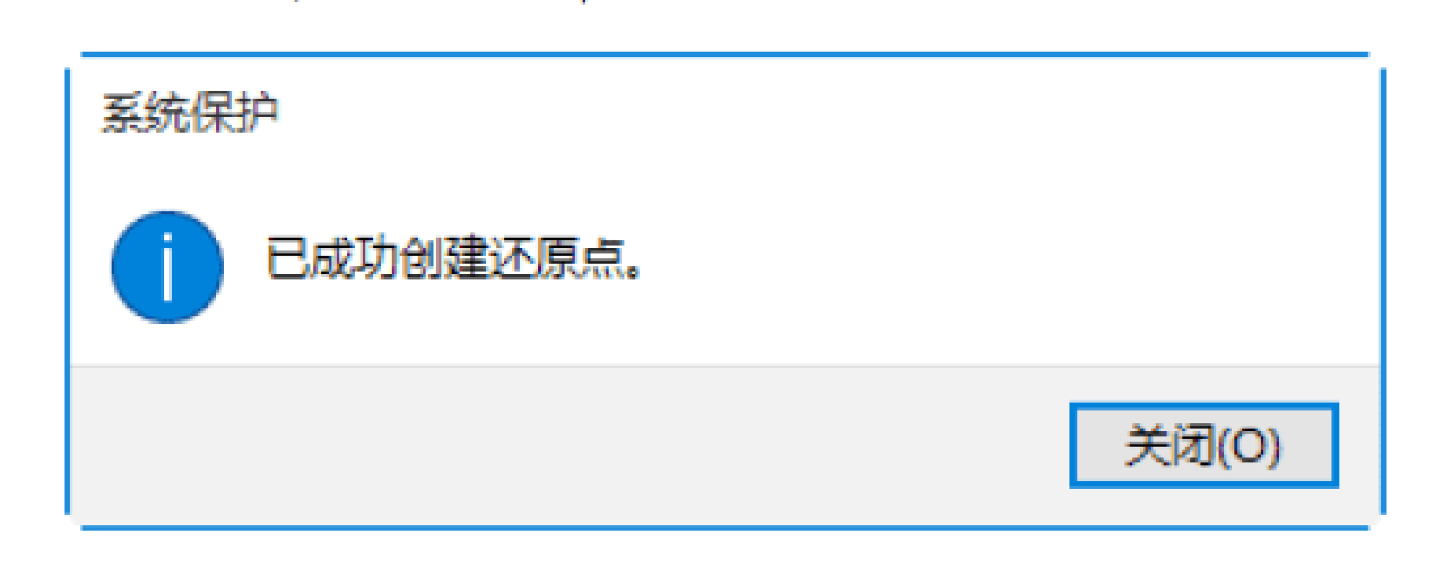
Step 02 弹出“创建还原点”对话框，在文本框中输入还原点的描述性信息，如下图所示。



Step 03 单击“创建”按钮，即可开始创建还原点，如下图所示。



Step 04 创建还原点的时间比较短，稍等片刻就可以了。创建完毕后，将打开“已成功创建还原点”提示信息，如下图所示，单击“关闭”按钮即可。



实战3：使用系统映像备份系统



Windows 10操作系统为用户提供了系统

映像的备份功能，使用该功能，用户可以备份整个操作系统。具体操作步骤如下。

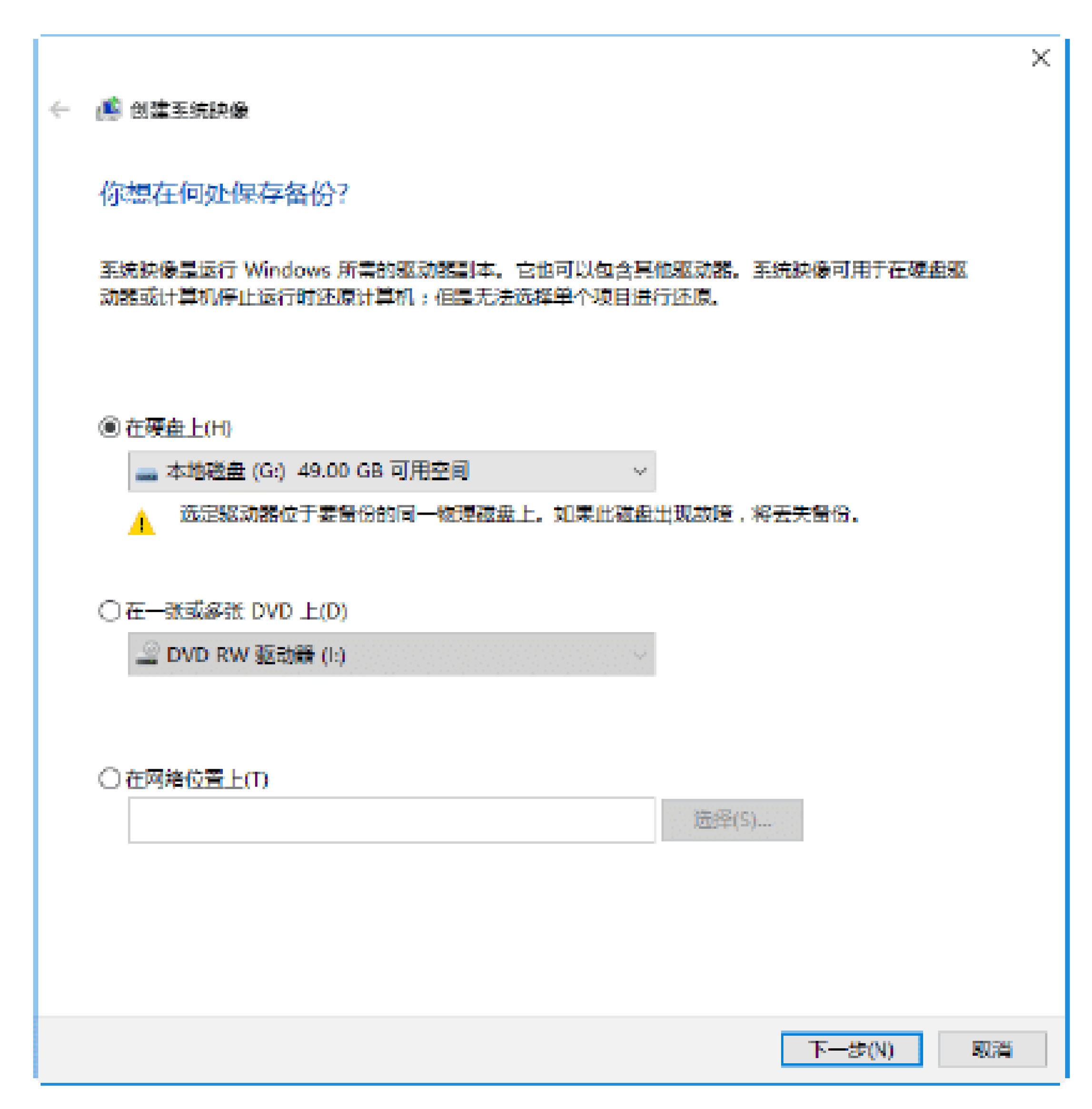
Step 01 在“控制面板”窗口中，单击“备份和还原（Windows）”超链接，如下图所示。



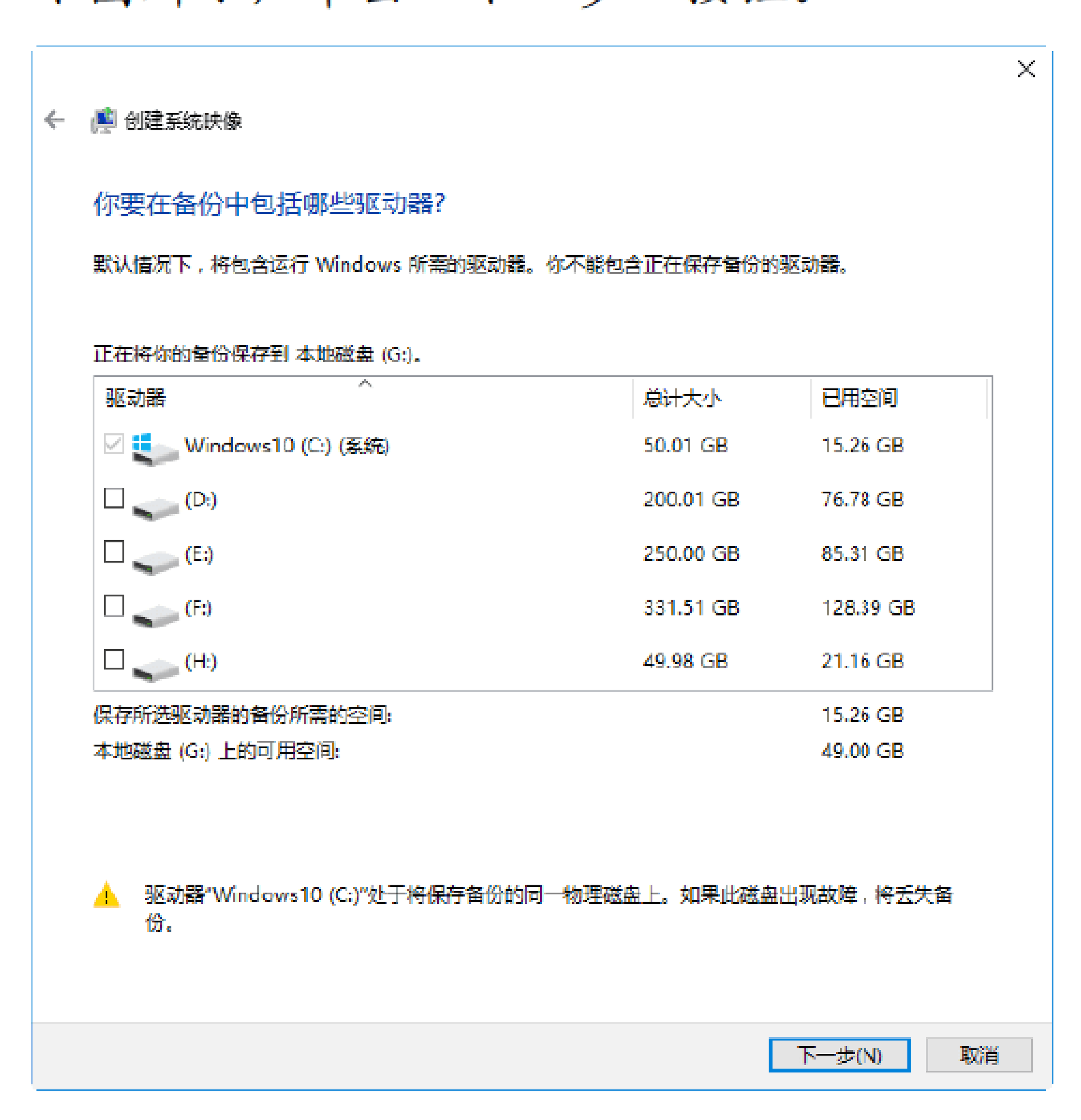
Step 02 弹出“备份和还原”窗口，如下图所示，单击“创建系统映像”链接。



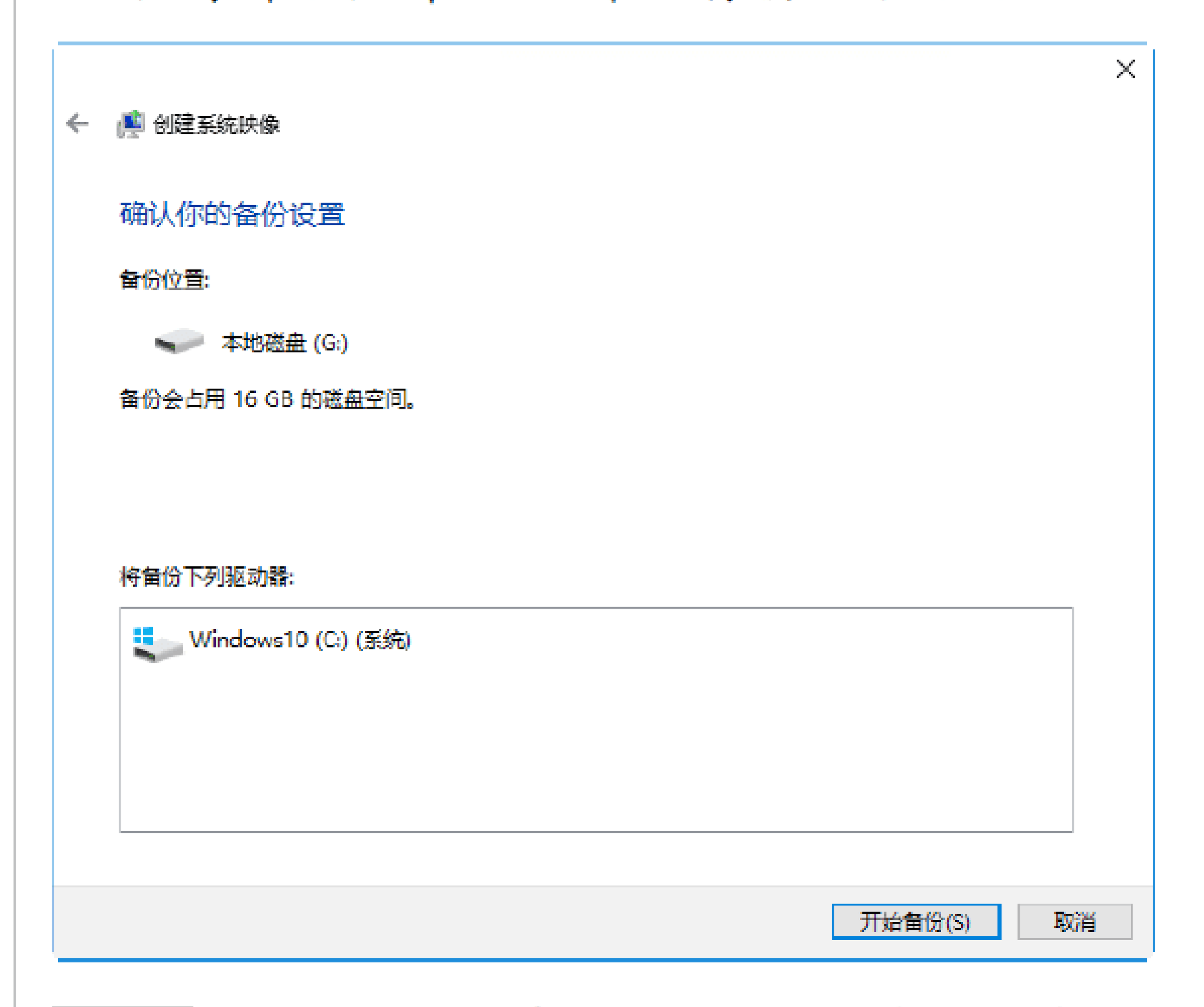
Step 03 弹出“你想在何处保存备份？”对话框，这里有3种类型的保存位置，包括在硬盘上、在一张或多张DVD上和在网络位置上，本实例选中“在硬盘上”单选按钮，如下图所示，单击“下一步”按钮。



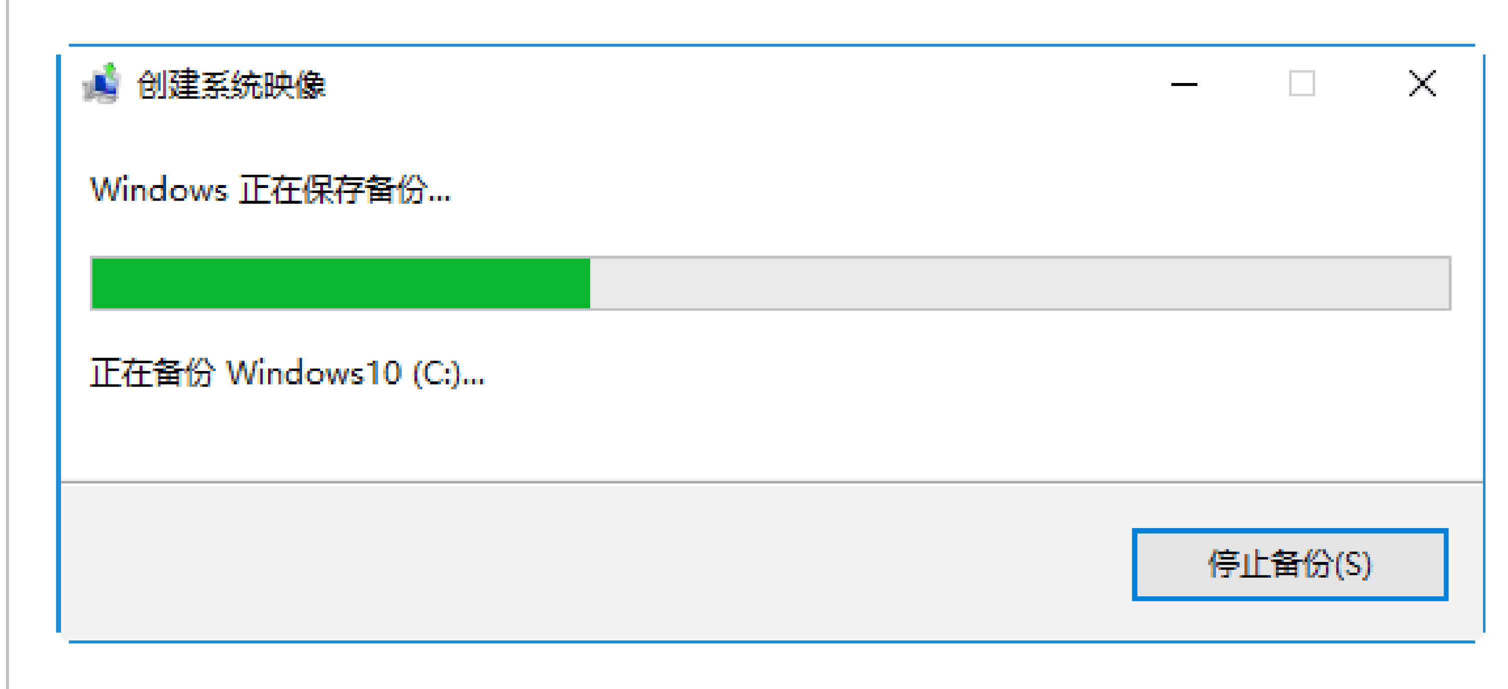
Step 04 弹出“你要在备份中包括哪些驱动器？”对话框，这里采用默认的选项，如下图所示，单击“下一步”按钮。



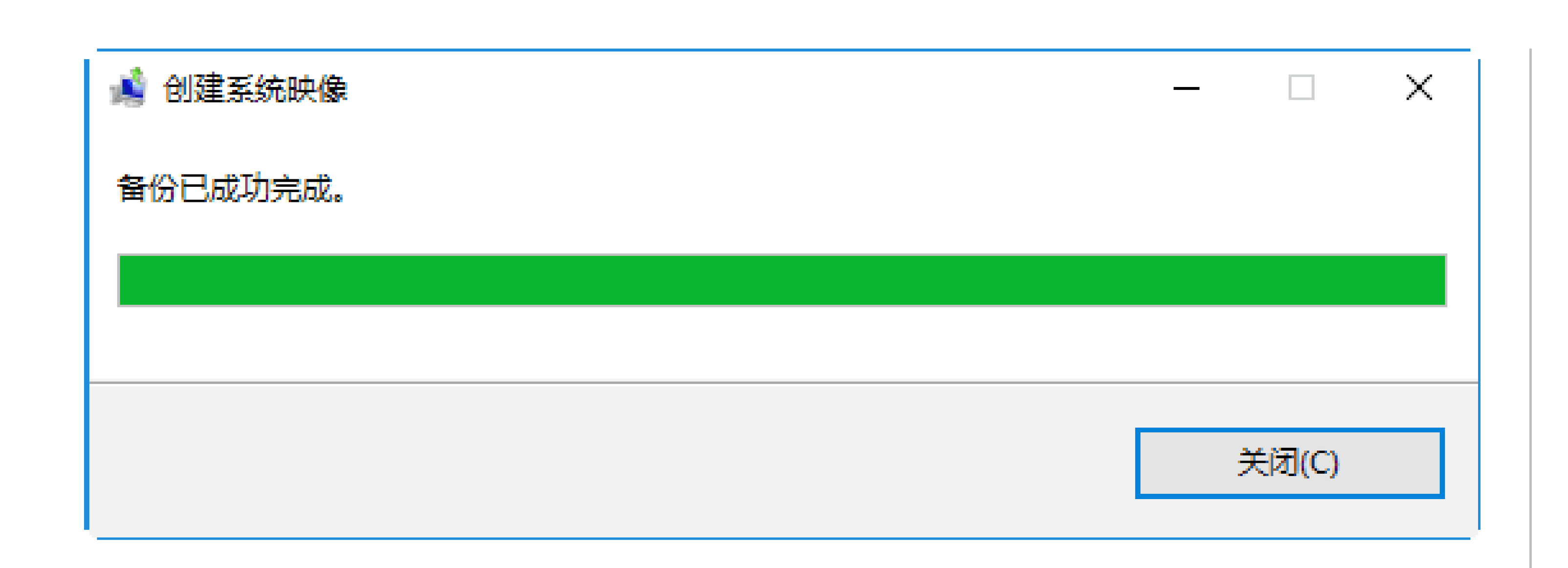
Step 05 弹出“确认你的备份设置”对话框，如下图所示，单击“开始备份”按钮。



Step 06 系统开始创建系统映像，并显示备份的进度，如下图所示。



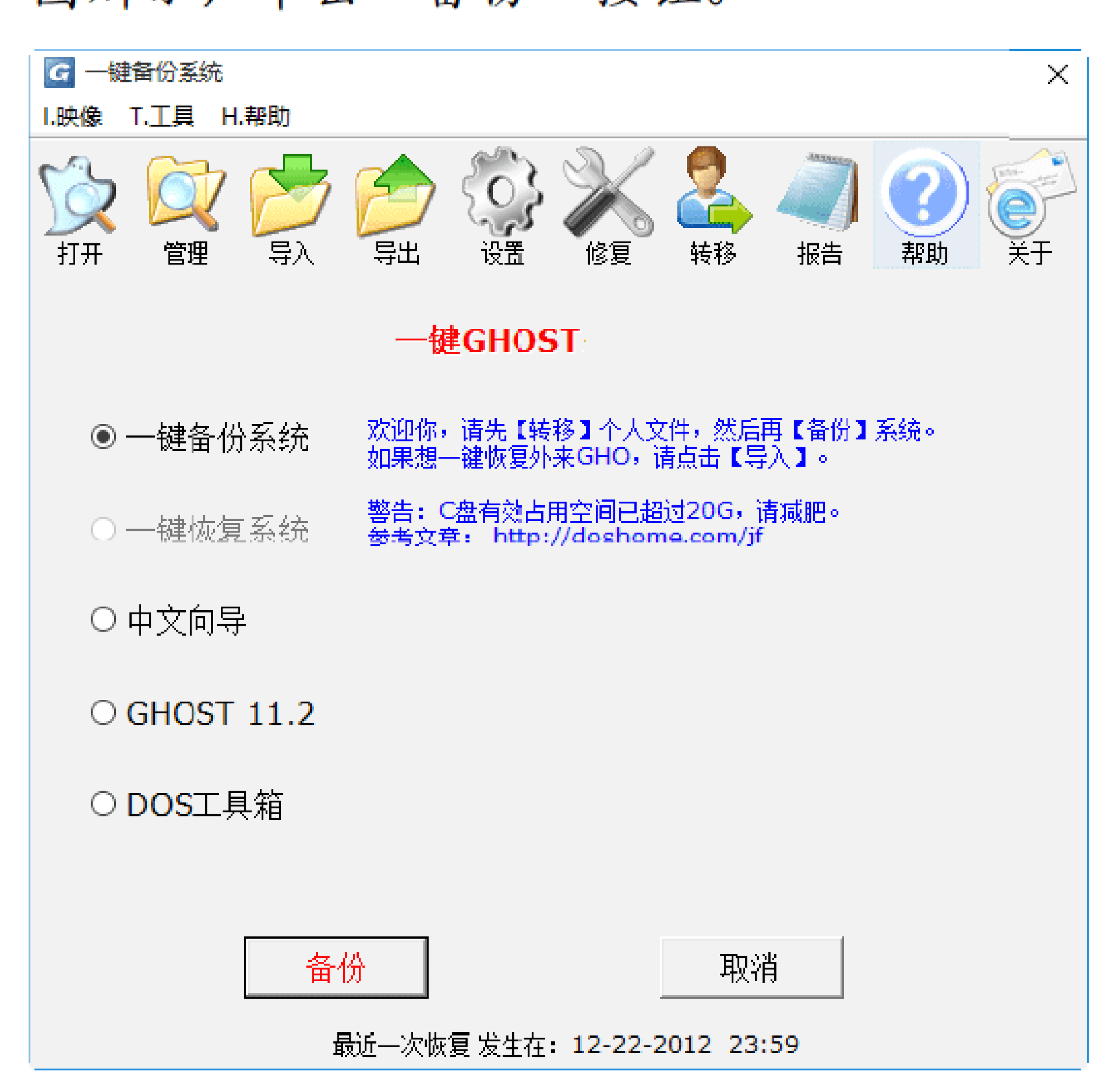
Step 07 备份完成后，单击“关闭”按钮即可，如下图所示。



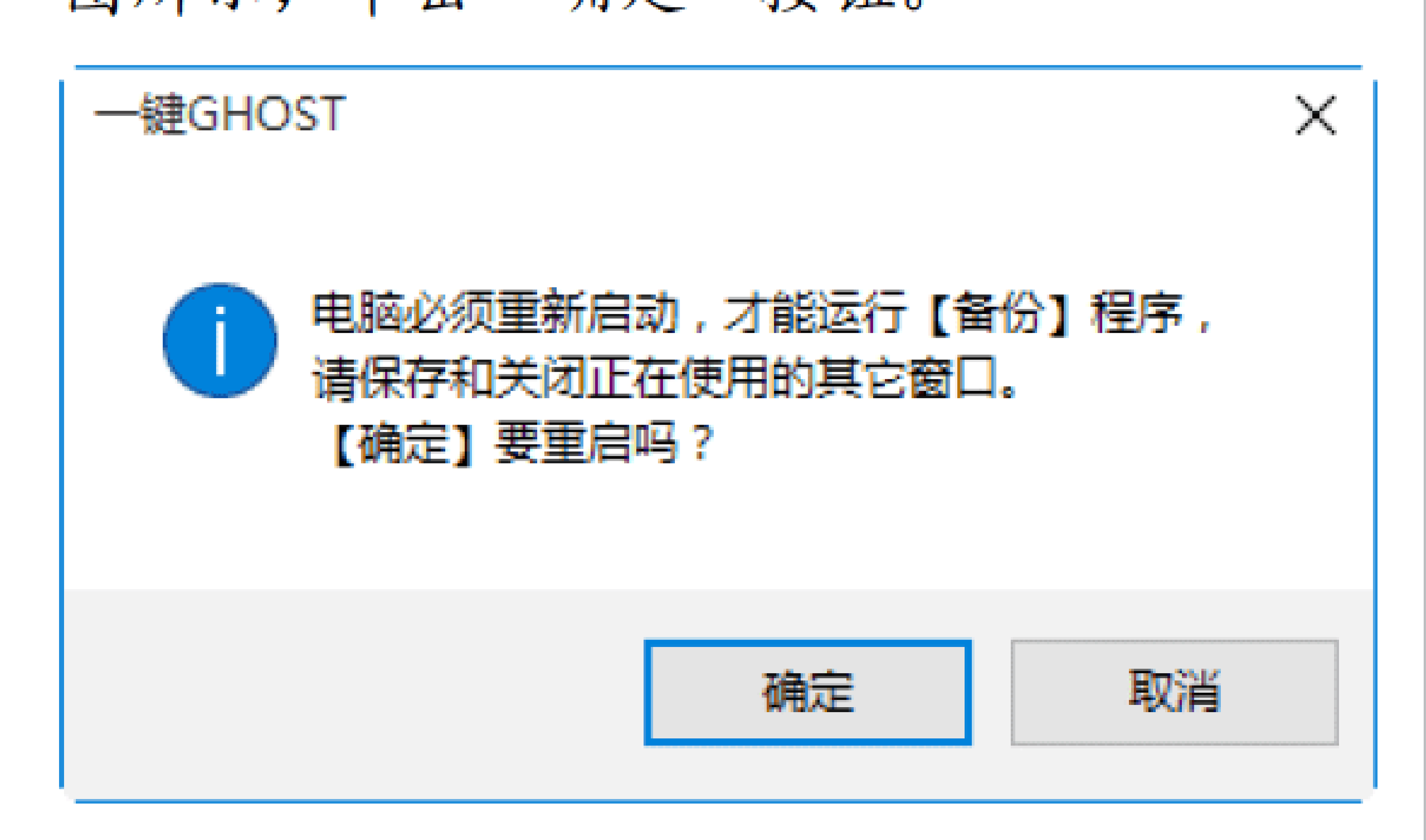
实战4：使用GHOST工具备份系统

一键GHOST是一个图形安装工具，主要包括一键备份系统、一键恢复系统、中文向导、GHOST、DOS工具箱等功能。使用一键GHOST备份系统的操作步骤如下。

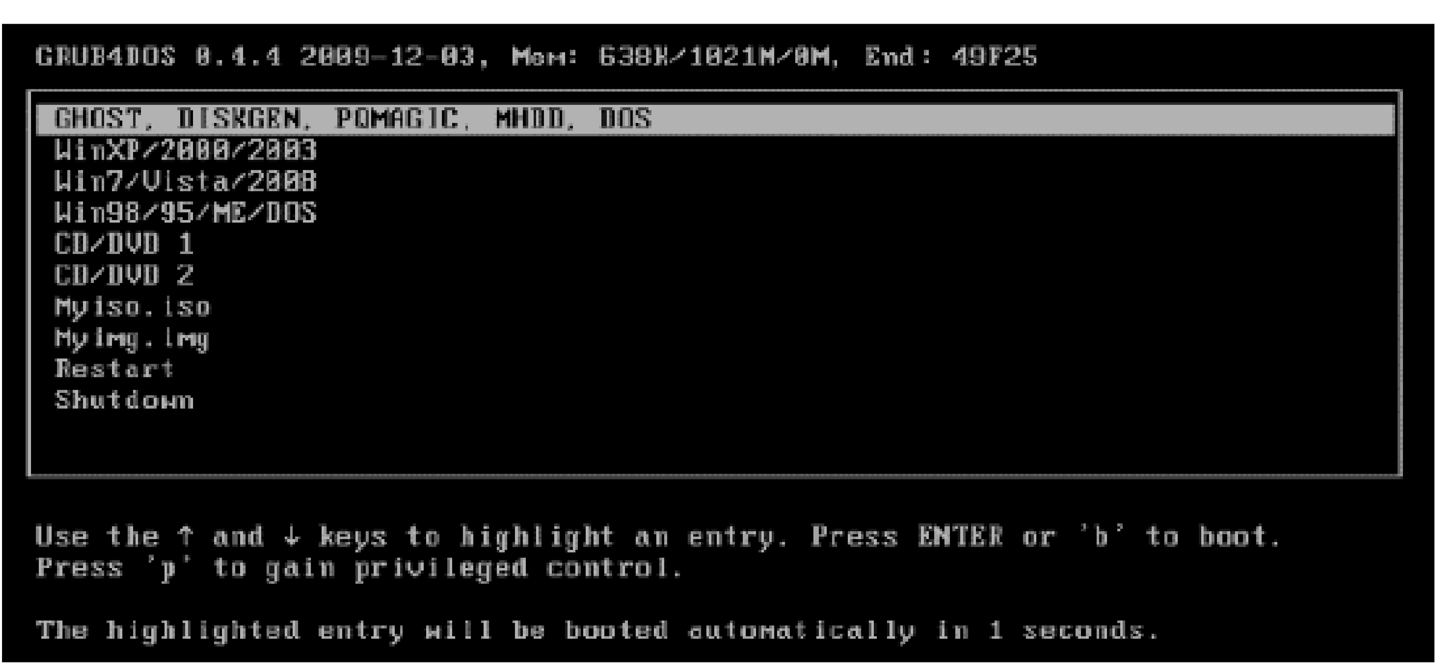
Step 01 下载并安装一键GHOST后，即可弹出“一键恢复系统”对话框，此时一键GHOST开始初始化。初始化完毕后，将自动选中“一键备份系统”单选按钮，如下图所示，单击“备份”按钮。



Step 02 弹出“一键GHOST”提示框，如下图所示，单击“确定”按钮。



Step 03 系统开始重新启动，并自动打开GRUB4DOS菜单，在其中选择第一个选项，表示启动一键GHOST，如下图所示。

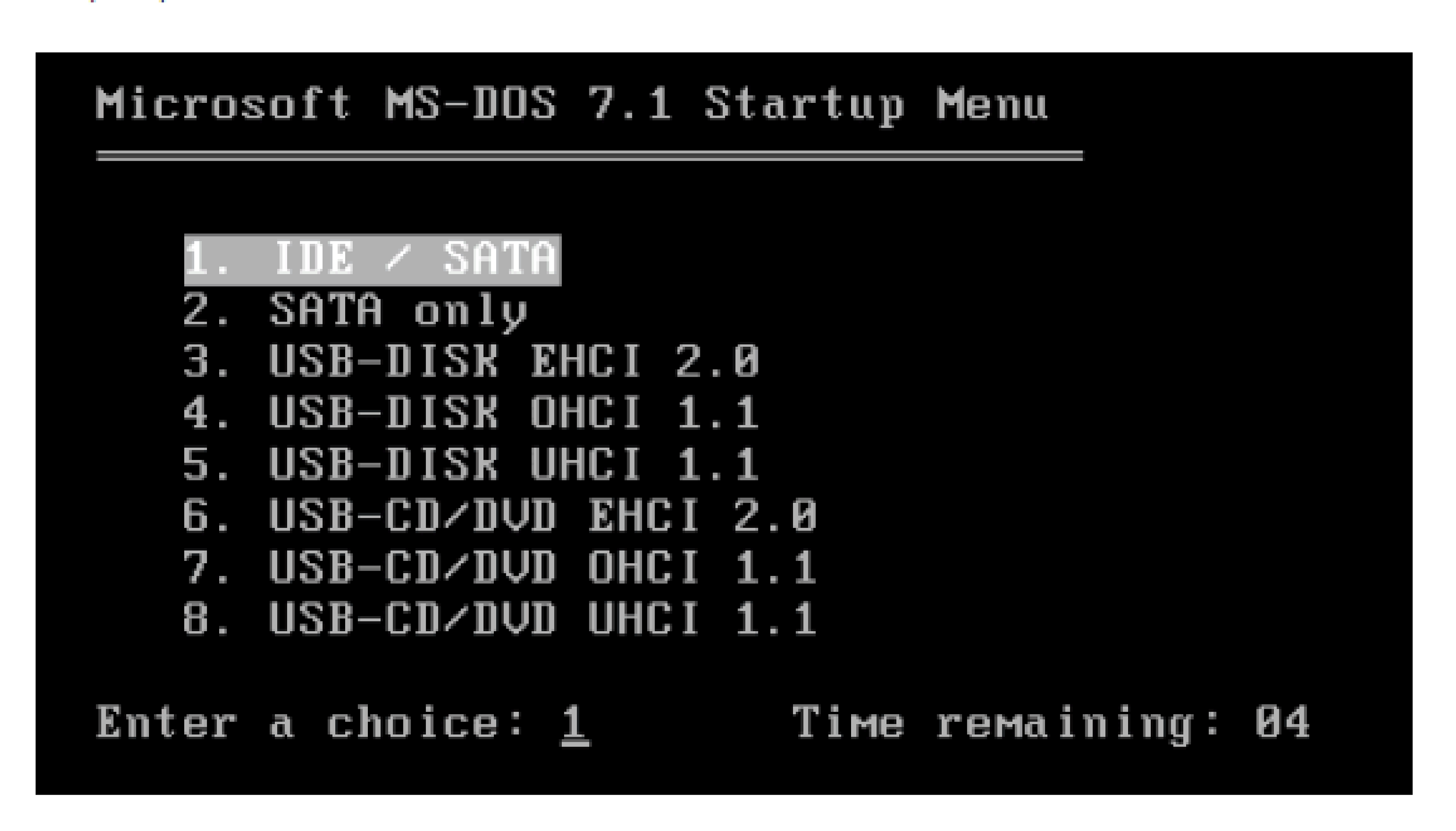




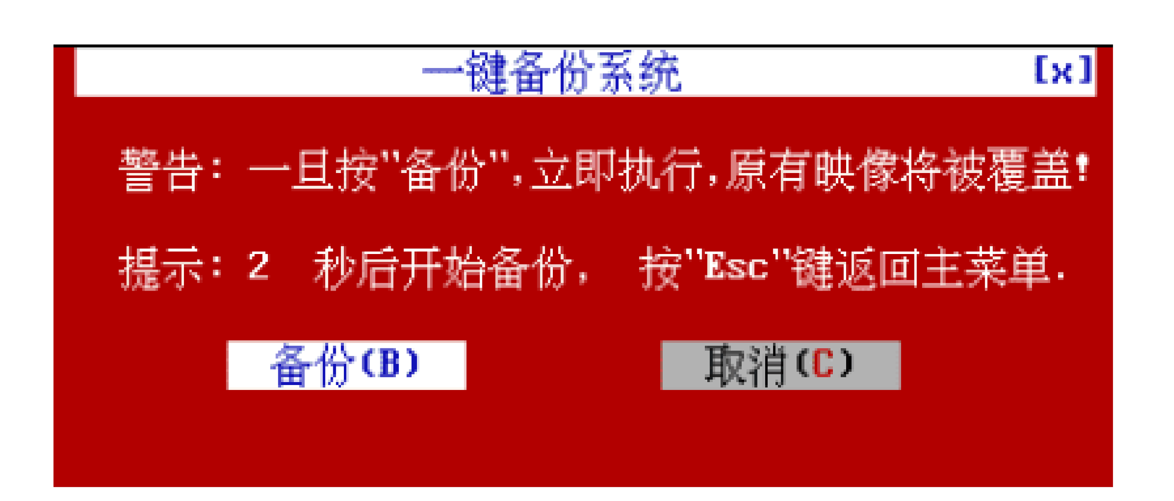
Step 04 系统自动选择完毕，接下来会弹出“MS-DOS一级菜单”界面，在其中选择第一个选项，表示在DOS安全模式下运行1KEY GHOST 11.2，如下图所示。



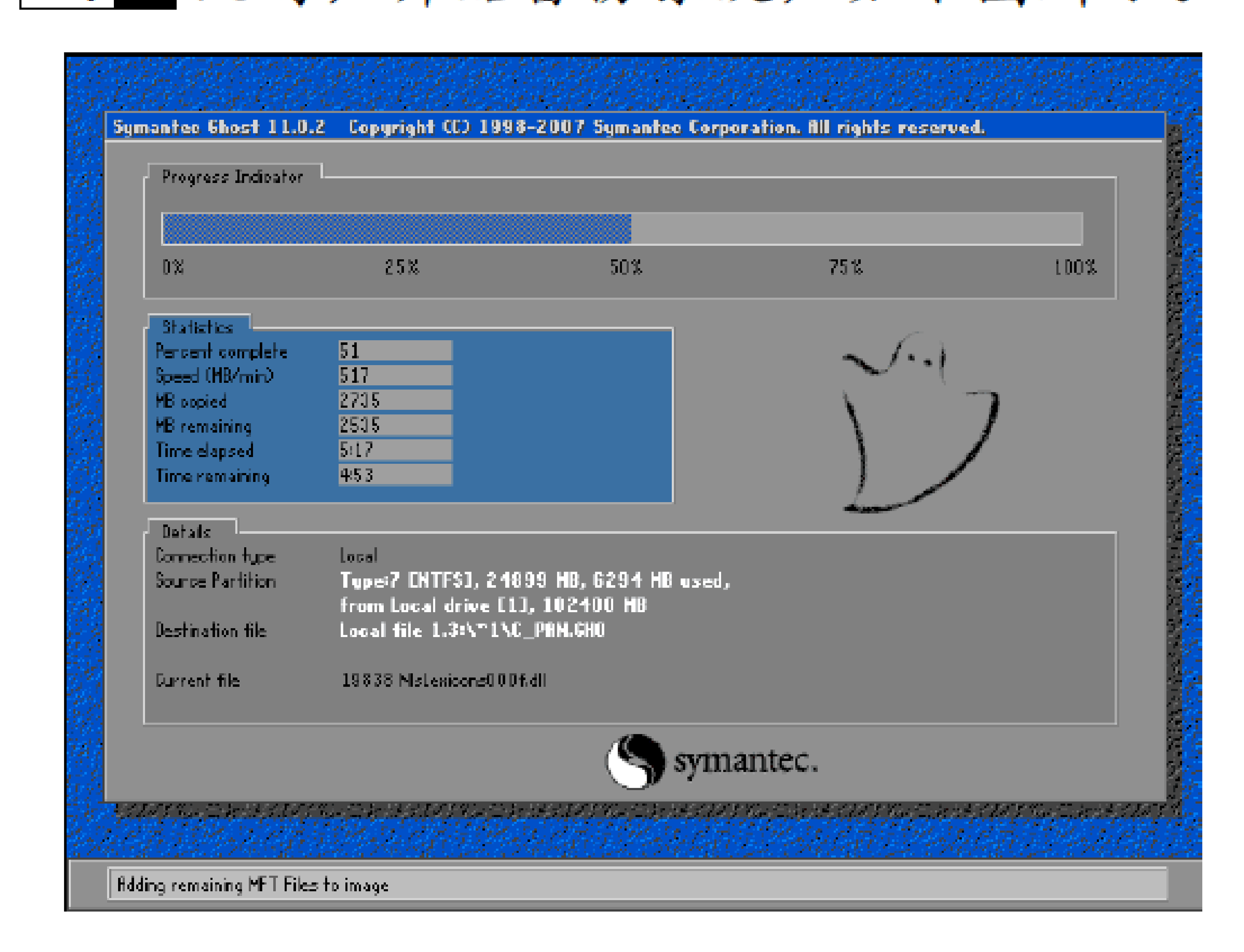
Step 05 选择完毕，接下来会弹出“MS-DOS二级菜单”界面，在其中选择第一个选项，表示支持IDE、SATA兼容模式，如下图所示。



Step 06 根据C盘是否存在映像文件，将会从主窗口自动进入“一键备份系统”警告窗口，提示用户开始备份系统，如下图所示。单击“备份”按钮。



Step 07 此时，开始备份系统，如下图所示。



14.3 还原崩溃后的操作系统

系统备份完成后，一旦系统出现严重的故障，即可还原系统到未出故障前的状态。

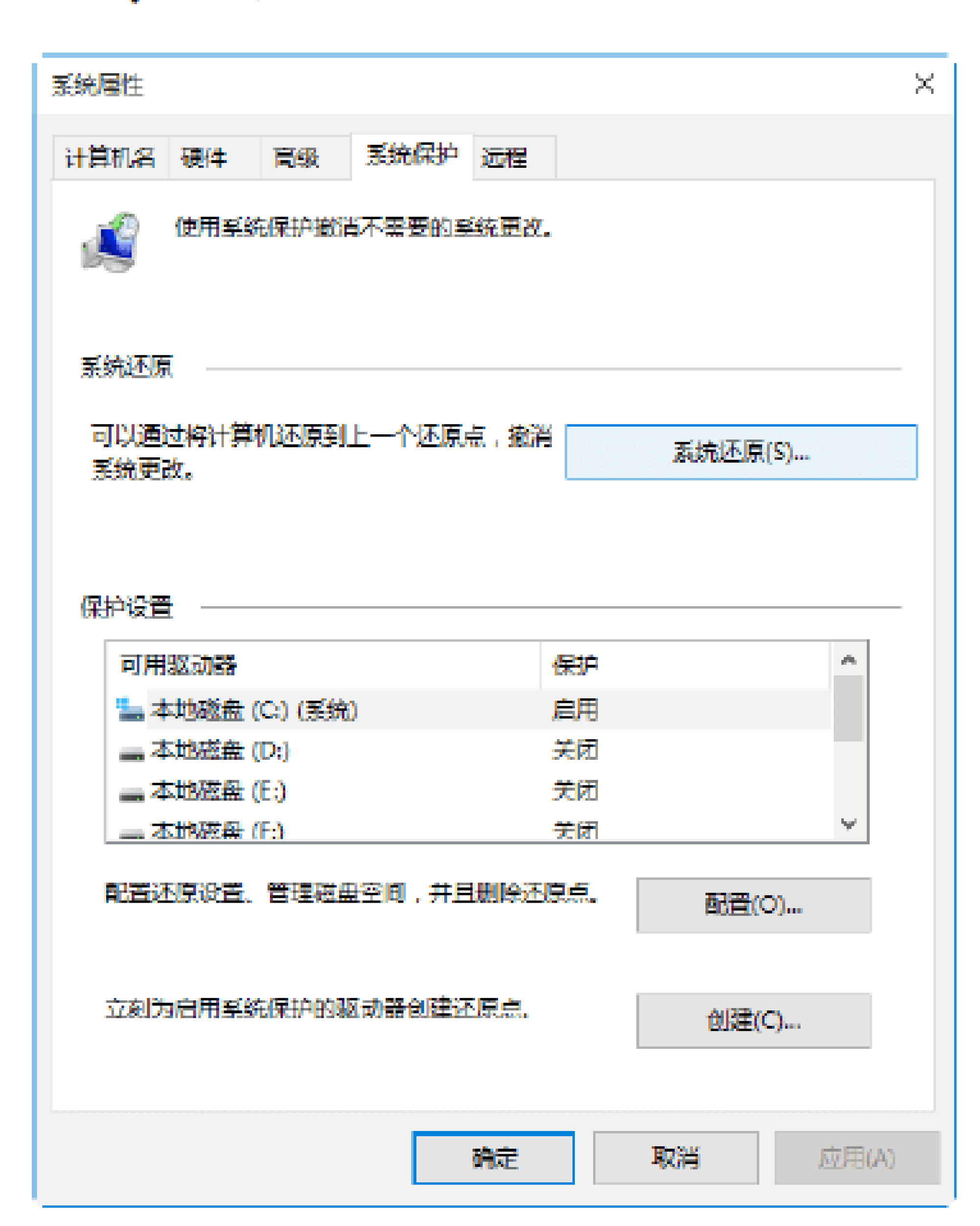


实战5：使用系统工具还原系统

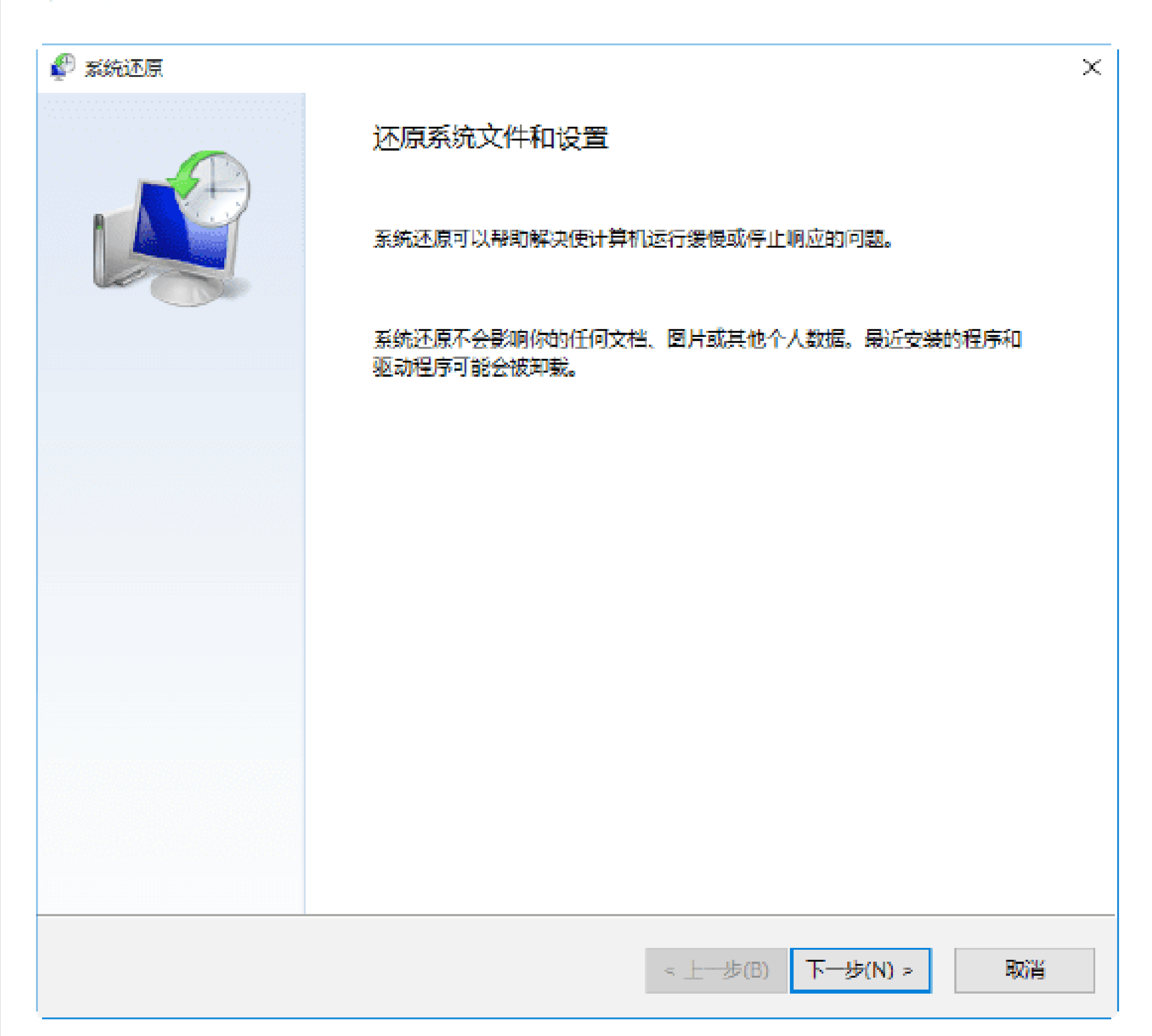
在为系统创建好还原点之后，一旦系统遭到病毒或木马的攻击，致使系统不能正常运行，这时就可以将系统恢复到指定还原点。

下面介绍如何还原到创建的还原点，具体操作步骤如下。

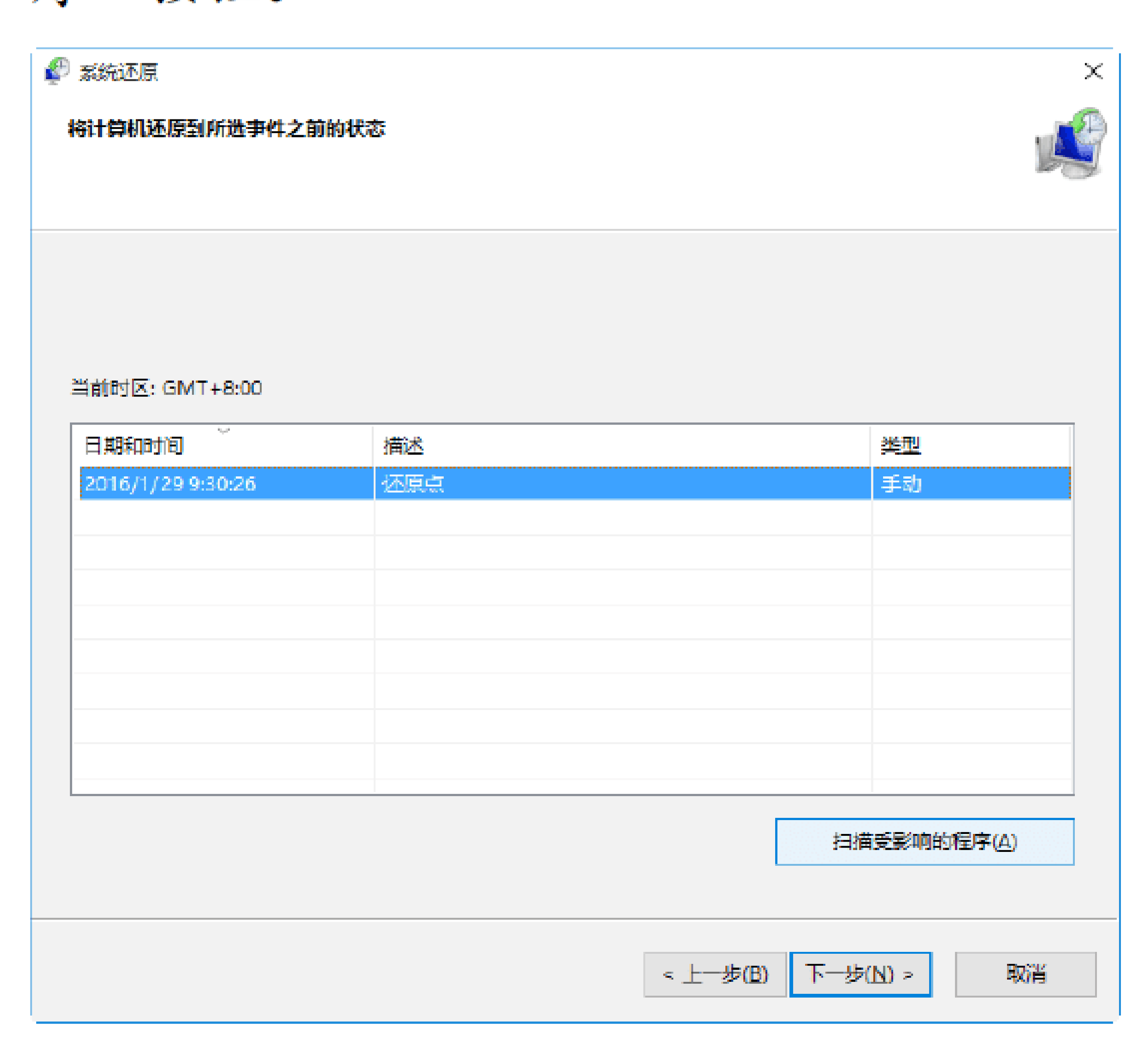
Step 01 在“系统属性”对话框中选择“系统保护”选项卡，如下图所示，然后单击“系统还原”按钮。



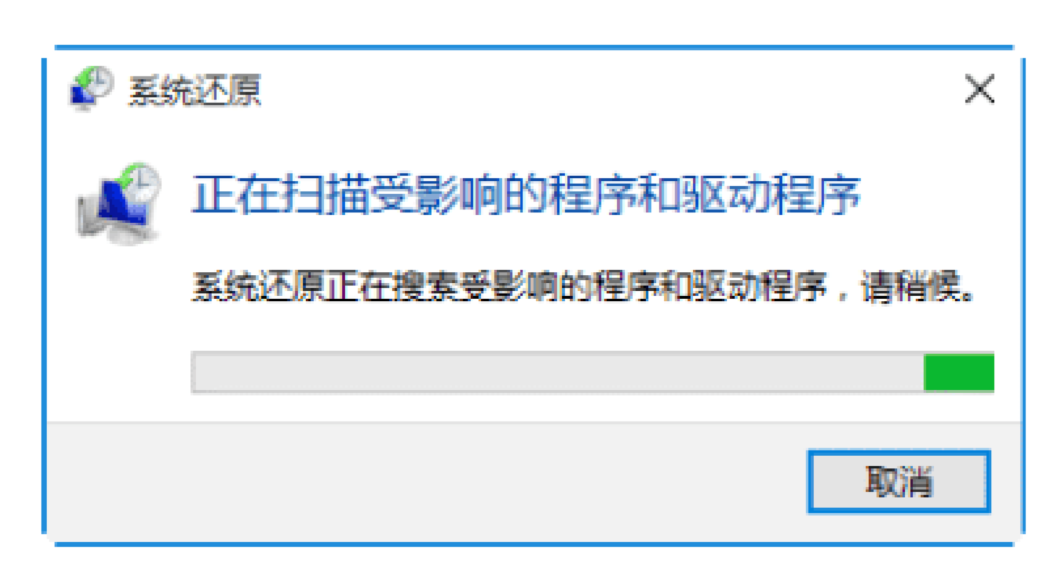
Step 02 即可弹出“还原系统文件和设置”对话框，如下图所示，单击“下一步”按钮。



Step 03 弹出“将计算机还原到所选事件之前的状态”对话框，如下图所示，选择合适的还原点，一般选择距离出现故障时间最近的还原点即可，单击“扫描受影响的程序”按钮。



Step 04 弹出“正在扫描受影响的程序和驱动程序”对话框，如下图所示。



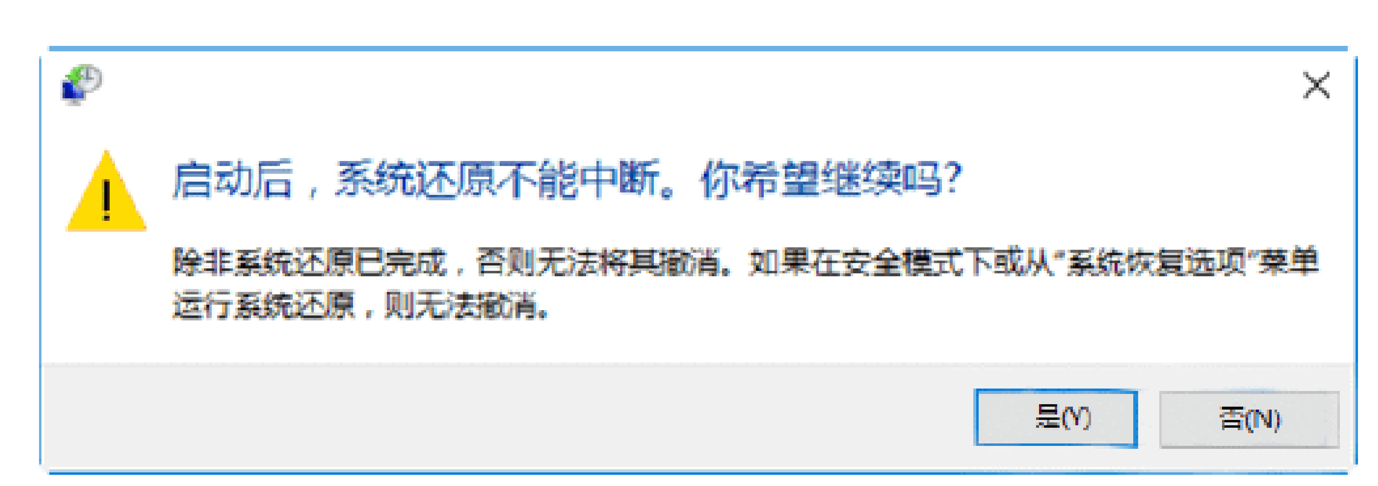
Step 05 稍等片刻，扫描完成后，将打开详细的被删除的程序和驱动信息，如下图所

示，用户可以查看所选择的还原点是否正确，如果不正确可以返回重新操作。



Step 06 单击"关闭"按钮，返回到"将计算机还原到所选事件之前的状态"对话框，确认还原点选择是否正确。如果还原点选择正确，则单击"下一步"按钮，弹出"确认还原点"对话框，如下图所示，如果确认操作正确，则单击"完成"按钮。

Step 07 打开提示框提示"启动后，系统还原不能中断，你希望继续吗？"，如下图所示，单击"是"按钮。计算机自动重启，还原操作会自动进行，还原完成后再次自动重启计算机，登录到桌面后，将会打开系统还原提示框提示"系统还原已成功完成。"，单击"关闭"按钮，即可完成将系统恢复到指定还原点的操作。



提示：如果还原后发现系统仍有问题，则可以选择其他的还原点进行还原。

实战6：使用GHOST工具还原系统



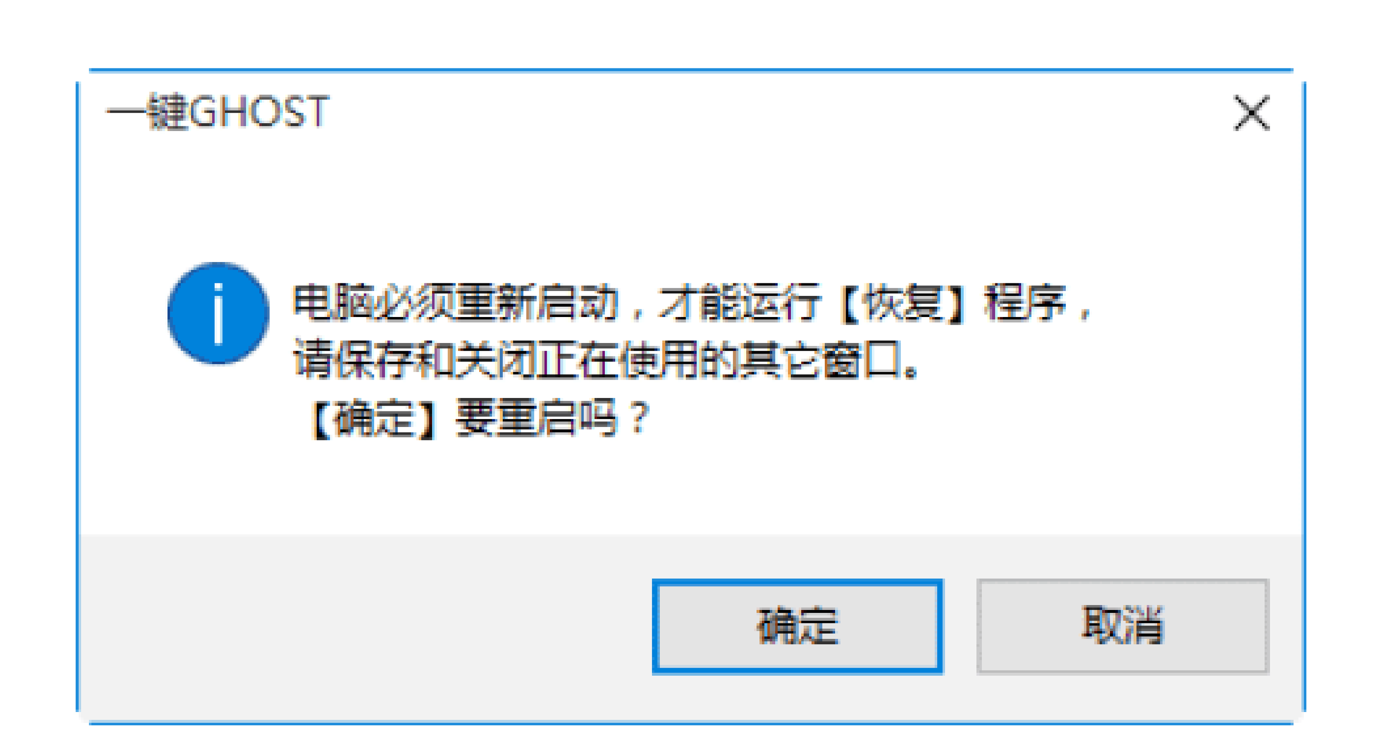
当系统分区中数据被损坏或系统遭受病毒和木马的攻击后，就可以利用GHOST的映像还原功能将备份的系统分区进行完全的还原，从而恢复系统。

使用一键GHOST还原系统的操作步骤如下。

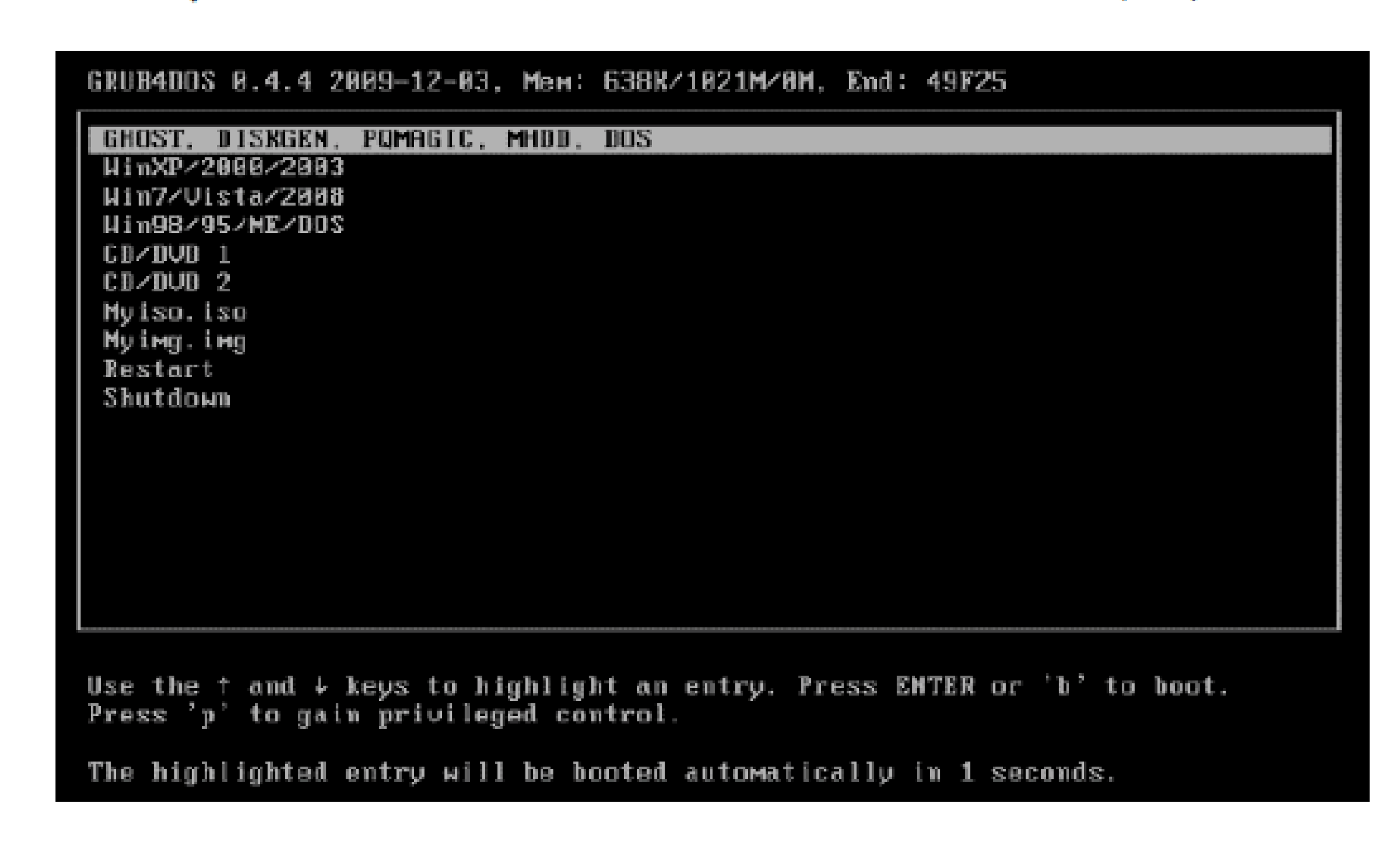
Step 01 在"一键GHOST"对话框中单击选中"一键恢复系统"单选按钮，如下图所示，单击"恢复"按钮。



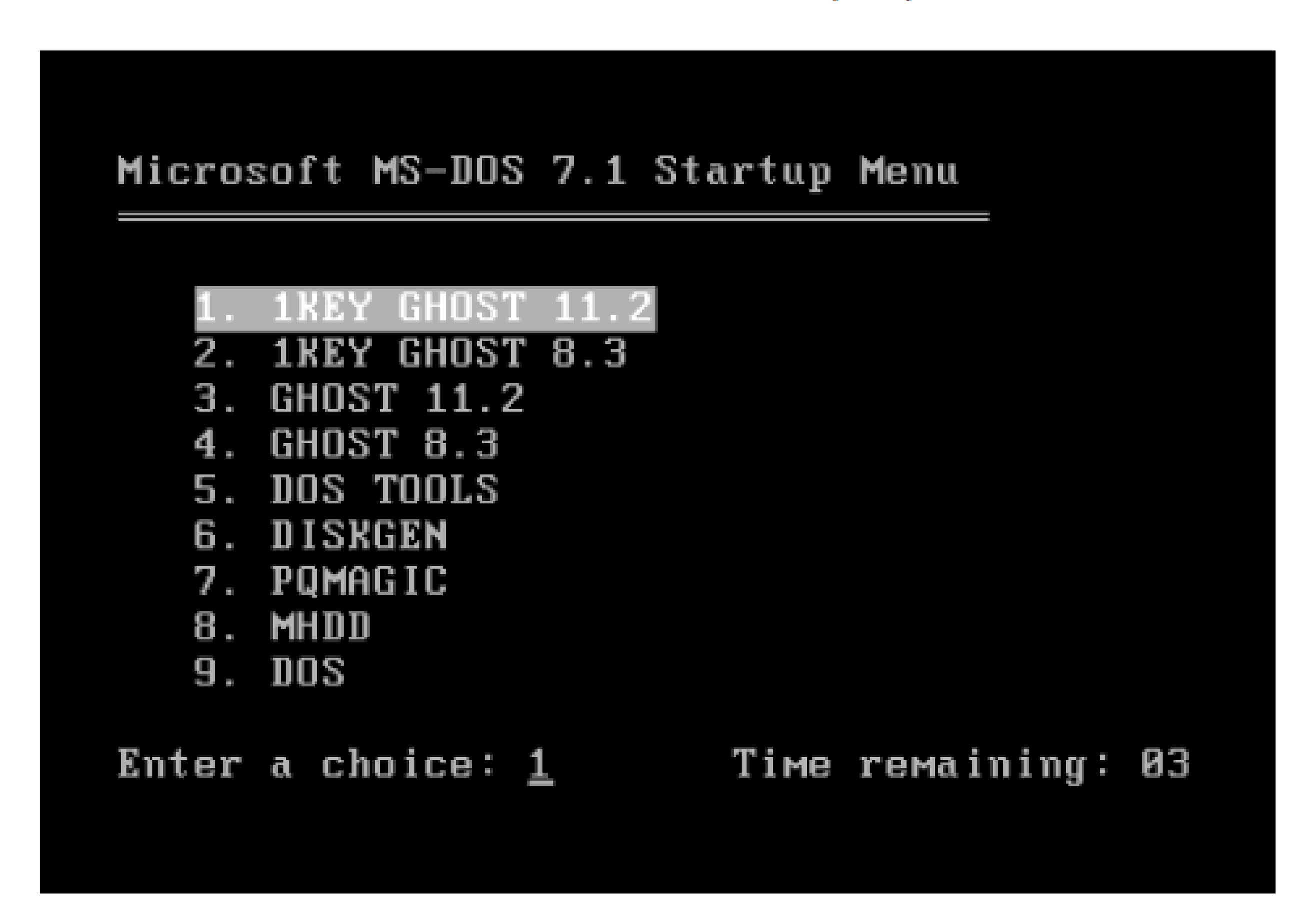
Step 02 弹出"一键GHOST"对话框，如下图所示，提示用户计算机必须重新启动，才能运行"恢复"程序，单击"确定"按钮。



Step 03 系统开始重新启动，并自动打开GRUB4DOS菜单，在其中选择第一个选项，表示启动一键GHOST，如下图所示。



Step 04 系统自动选择完毕，接下来会弹出“MS-DOS一级菜单”界面，在其中选择第一个选项，表示在DOS安全模式下运行1KEY GHOST 11.2，如下图所示。

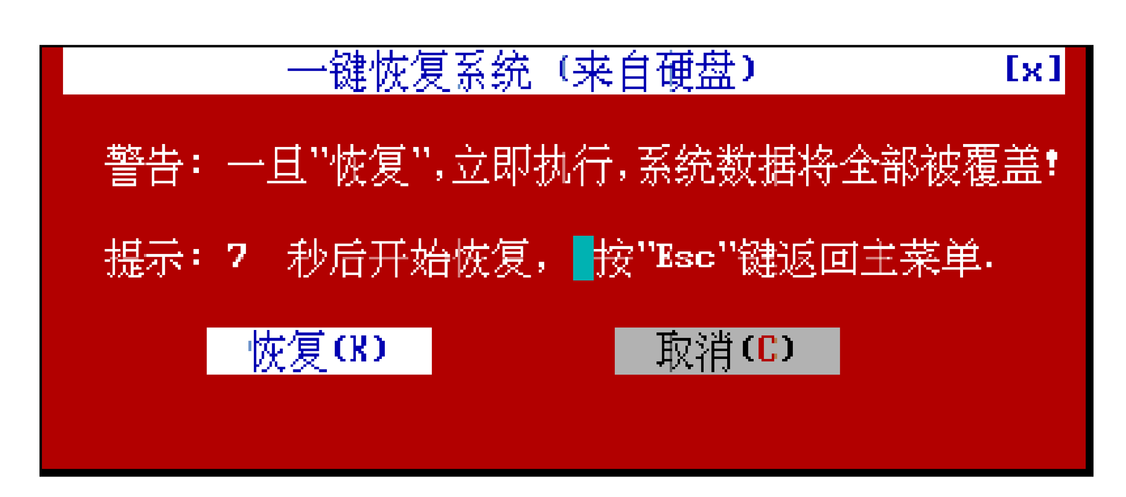


Step 05 选择完毕，接下来会弹出“MS-DOS二级菜单”界面，在其中选择第一个选项，表示支持IDE、SATA兼容模式，如下图所示。

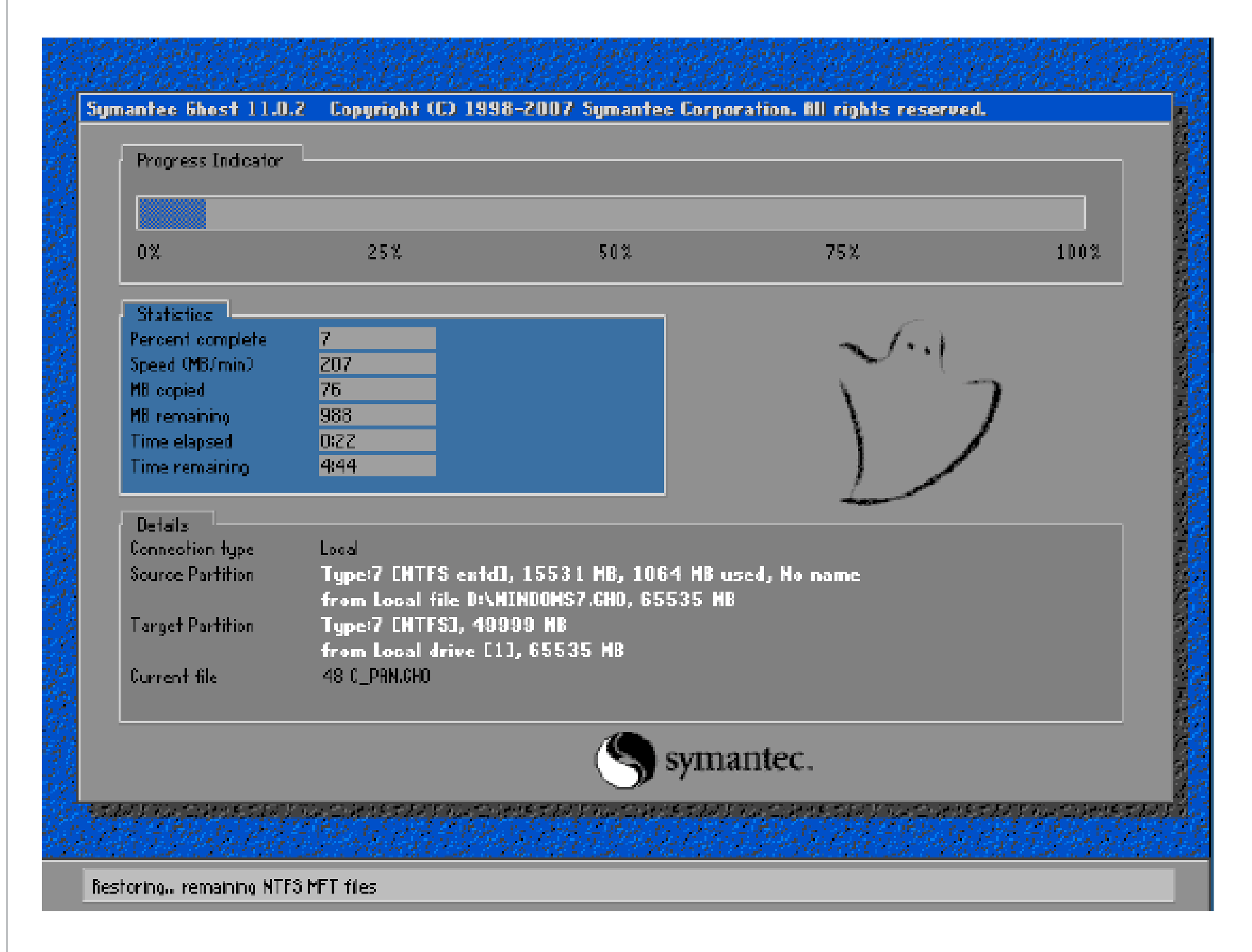




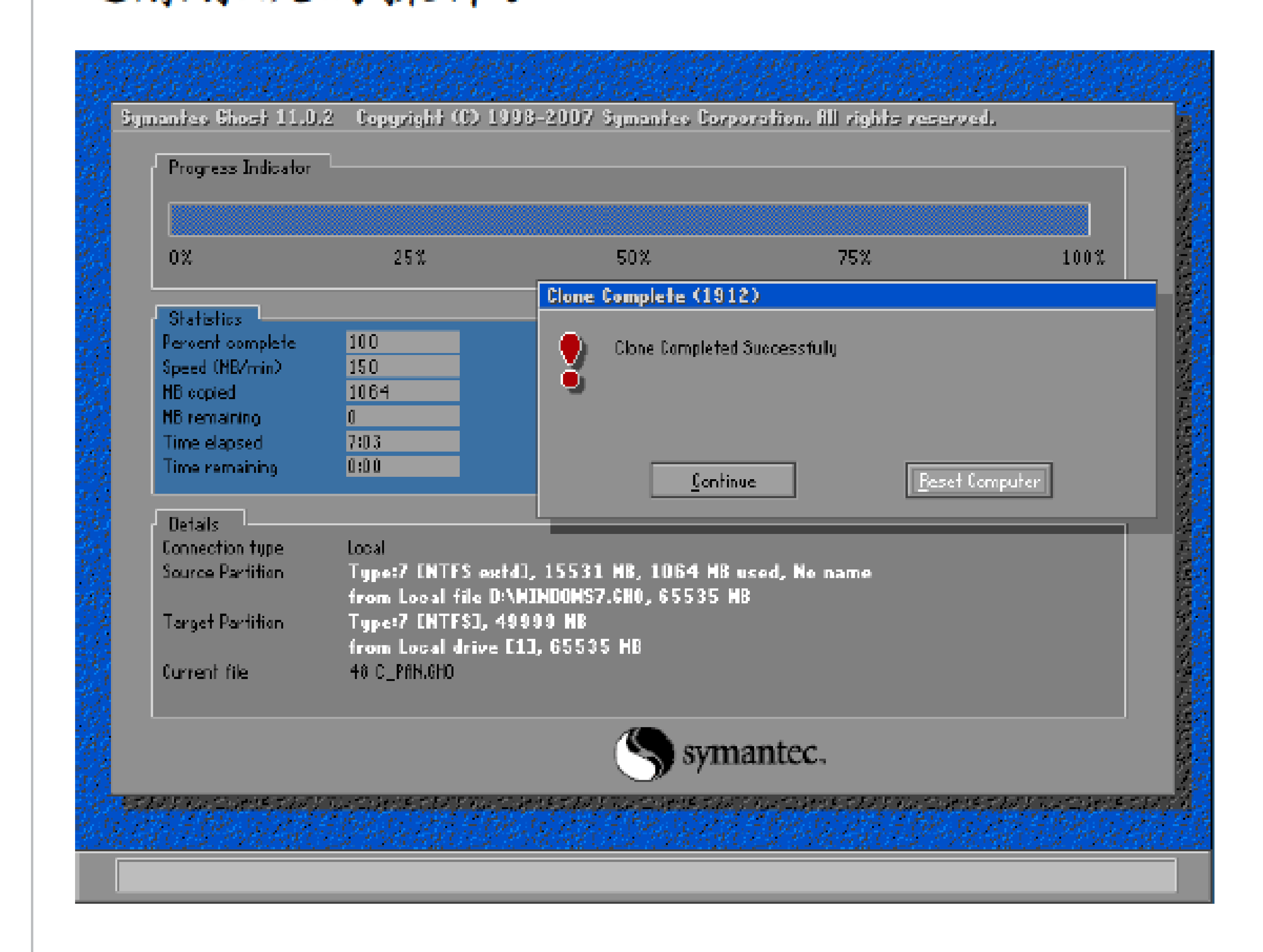
Step 06 根据C盘是否存在映像文件，将会从主窗口自动进入“一键恢复系统”警告窗口，提示用户开始恢复系统，如下图所示。单击“恢复”按钮，即可开始恢复系统。



Step 07 此时，开始恢复系统，如下图所示。



Step 08 在系统还原完毕后，将打开一个信息提示框，提示用户恢复成功，单击Reset Computer按钮重启计算机，选择从硬盘启动，即可将系统恢复到以前的系统，如下图所示。至此，就完成了使用GHOST工具还原系统的操作。

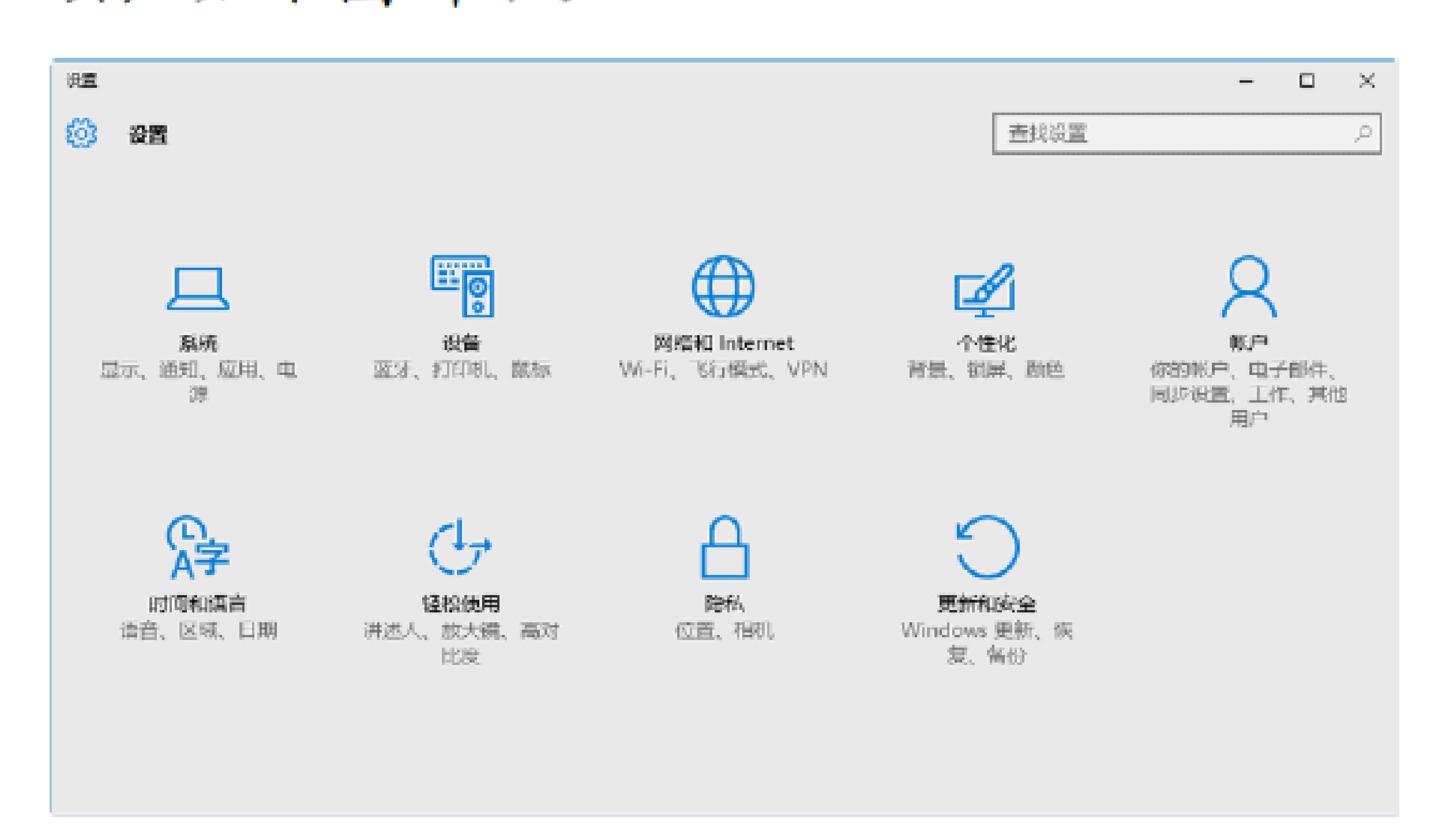


实战7：使用系统映像还原系统

完成系统映像的备份后，如果系统出现问题，可以利用映像文件进行还原操

作。具体操作步骤如下。

Step 01 在桌面上右击“开始”按钮，在打开的快捷菜单中选择“设置”选项，弹出“设置”窗口，选择“更新和安全”选项，如下图所示。



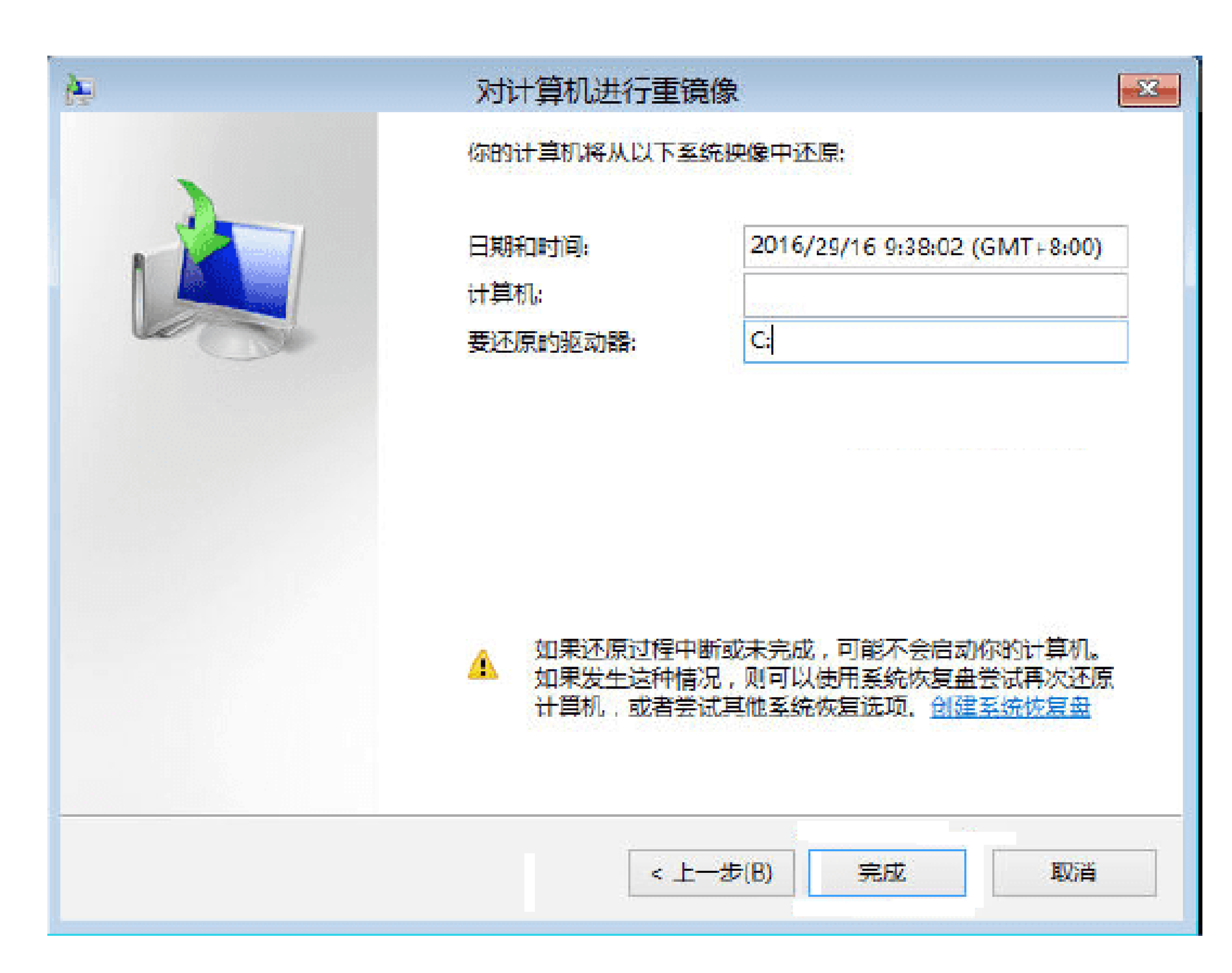
Step 02 弹出“更新和安全”窗口，如下图所示，在左侧列表中选择“恢复”选项，在右侧窗口单击“立即启动”按钮。



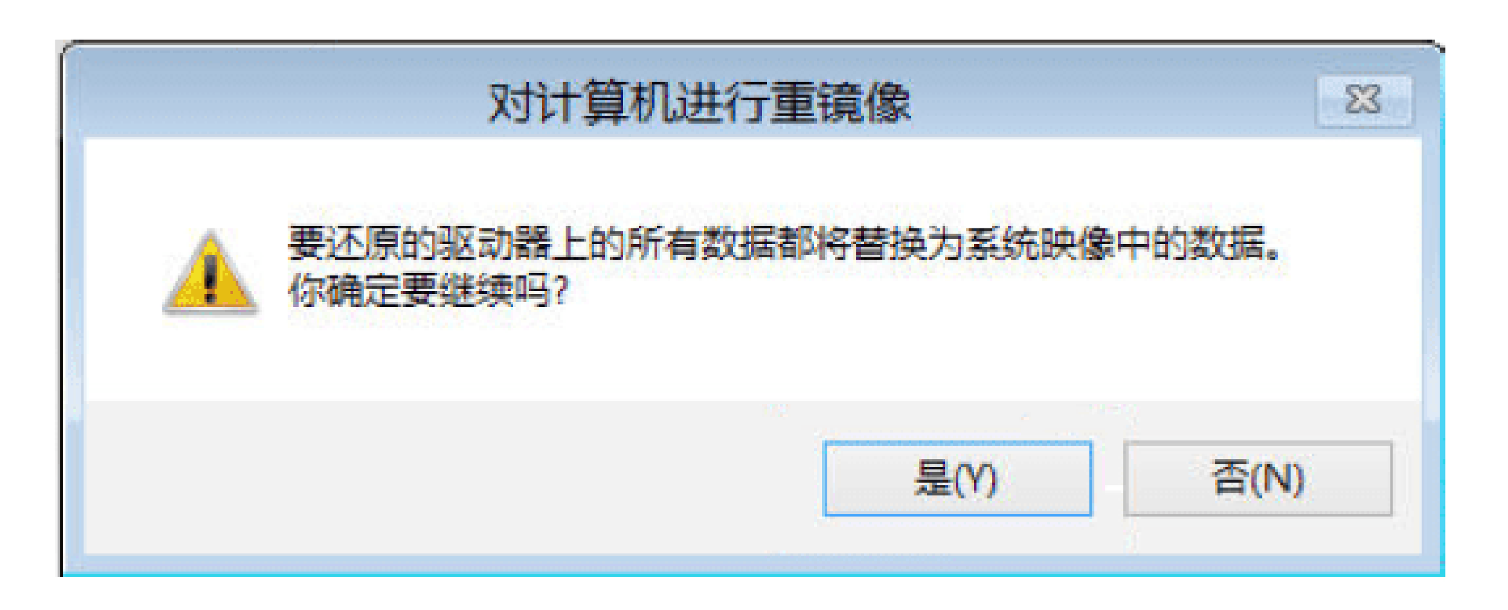
Step 03 弹出“选择其他的还原方式”对话框，如下图所示，采用默认设置，单击“下一步”按钮。



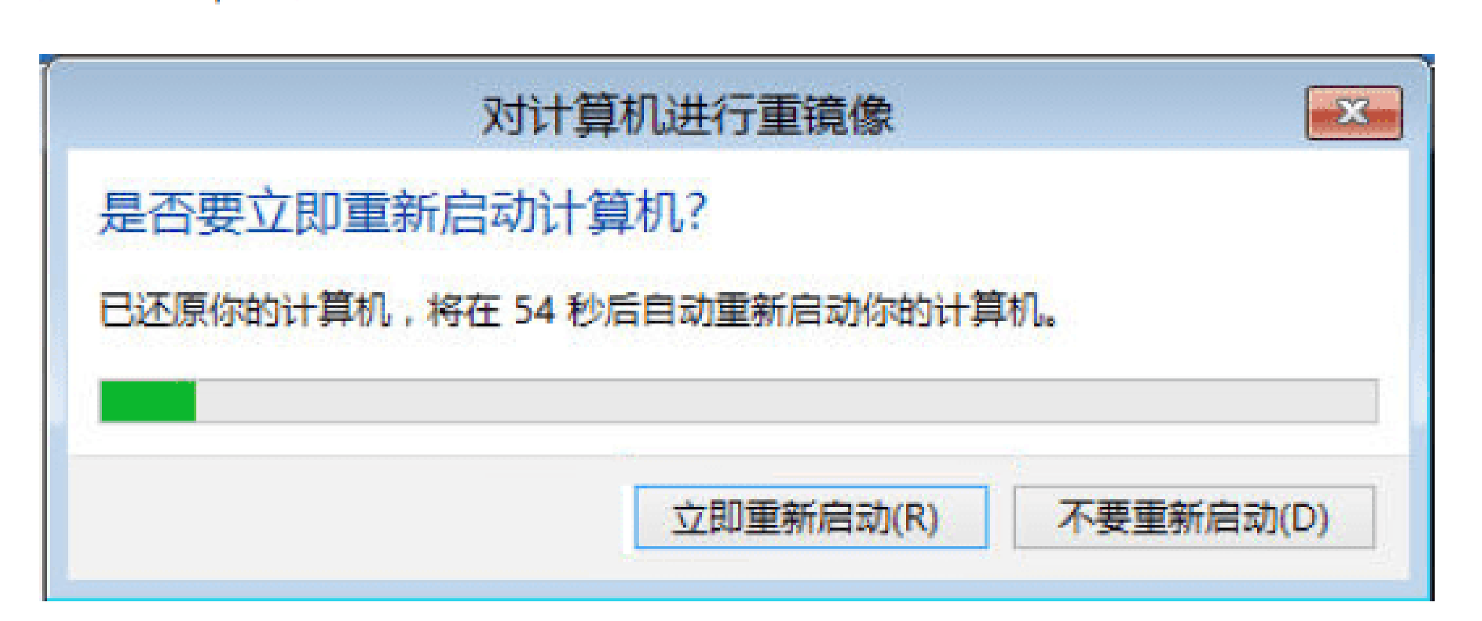
Step 04 弹出“你的计算机将从以下系统映像中还原”对话框，如下图所示，单击“完成”按钮。



Step 05 打开提示信息对话框，如下图所示，单击“是”按钮。



Step 06 系统映像的还原操作完成后，弹出“是否要立即重新启动计算机？”对话框，如下图所示，单击“立即重新启动”按钮即可。



14.4　重置崩溃后的操作系统

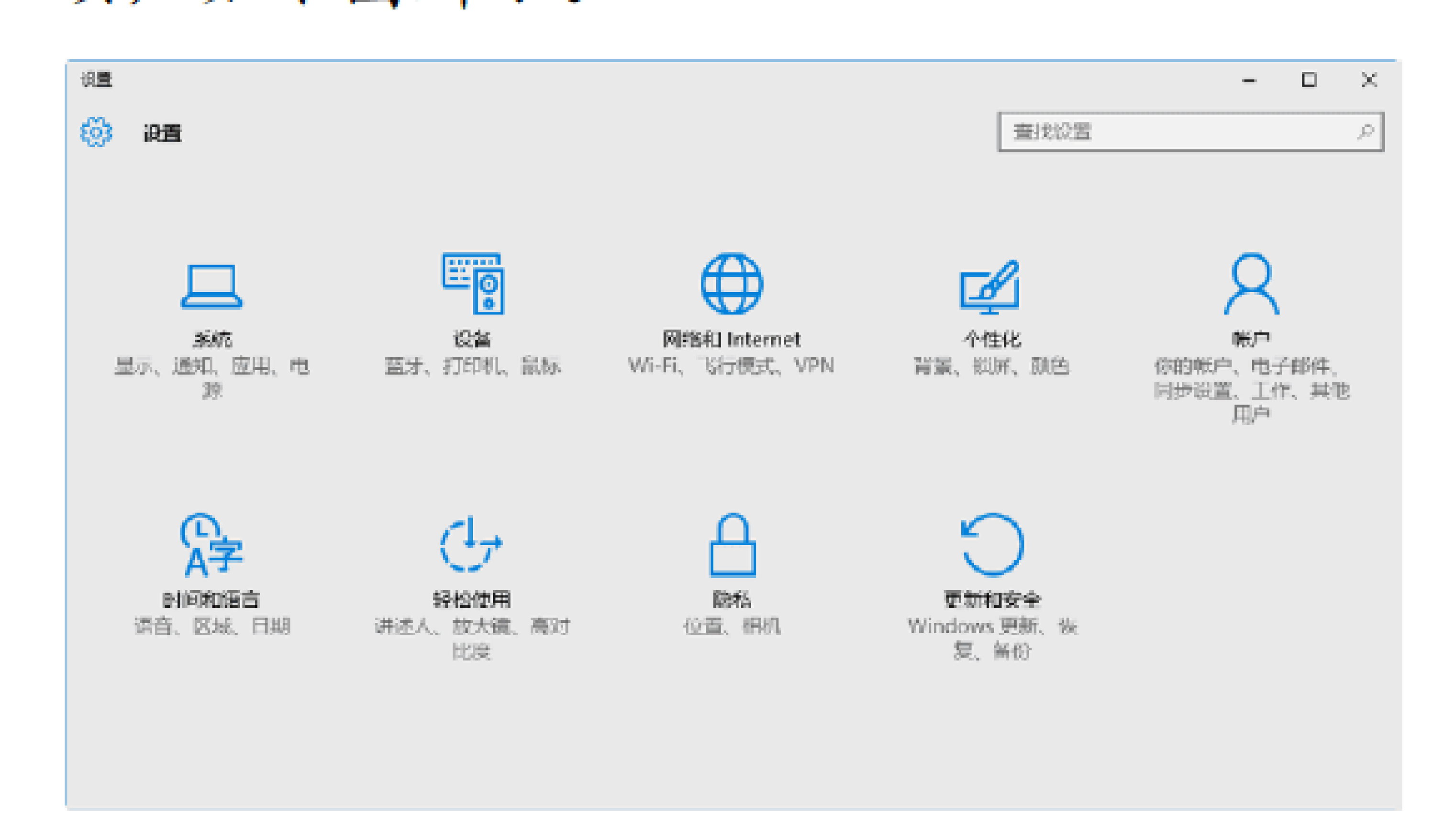
对于系统文件出现丢失或者文件异常的情况，可以通过重置的方法来修复系统。重置计算机可以在计算机出现问题时方便地将系统恢复到初始状态，而不需要重装系统。

实战8：在可开机情况下重置计算机



在可以正常开机并进入Windows 10操作系统后，重置计算机的具体操作步骤如下。

Step 01 在桌面上右击“开始”按钮，在打开的快捷菜单中选择“设置”选项，弹出“设置”窗口，选择“更新和安全”选项，如下图所示。



Step 02 弹出“更新和安全”窗口，如下图所示，在左侧列表中选择“恢复”选项，在右侧窗口单击“立即重启”按钮。



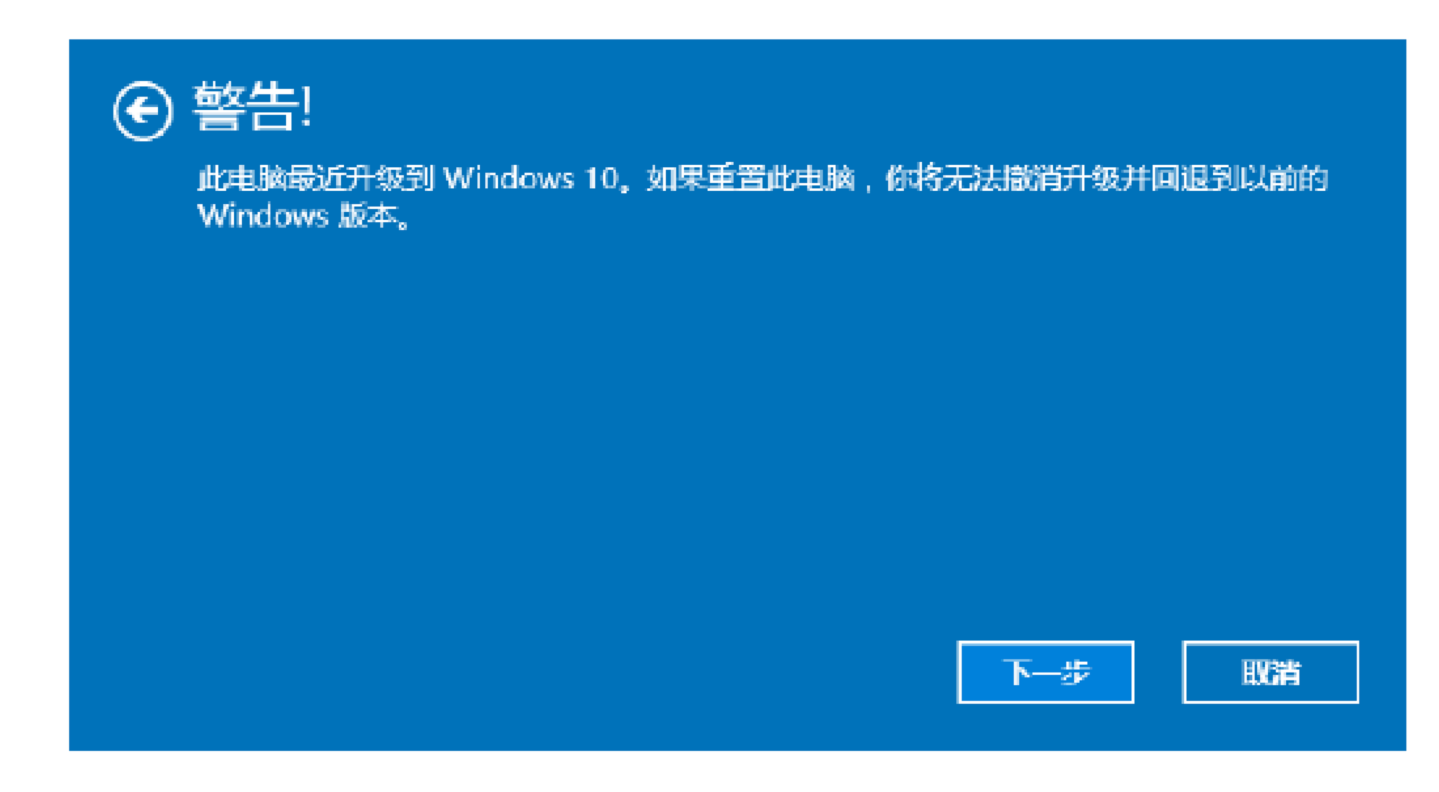
Step 03 弹出“选择一个选项”界面，如下图所示，单击选择“保留我的文件”选项。



Step 04 弹出“将会删除你的应用”界面，如下图所示，单击“下一步”按钮。



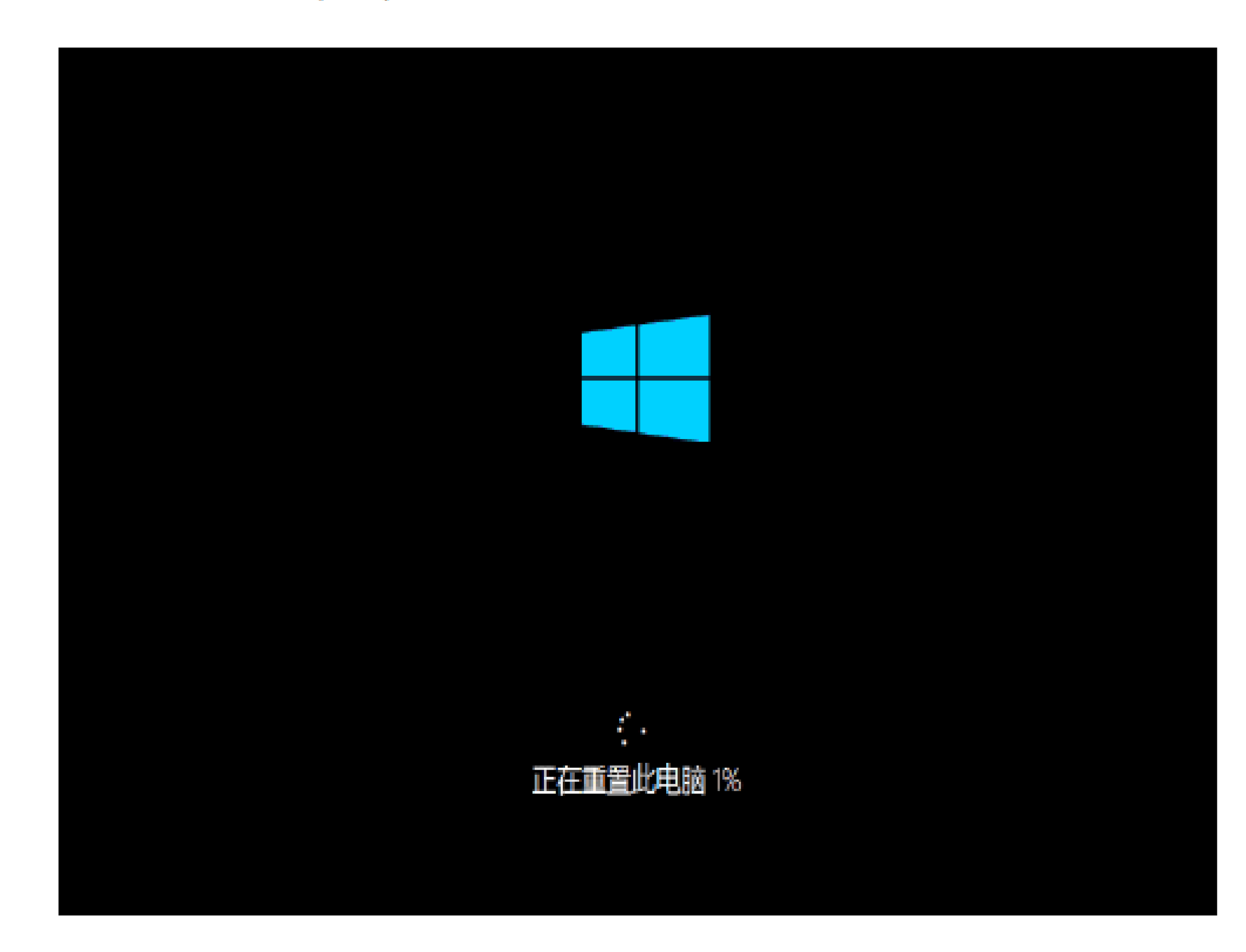
Step 05 弹出“警告”界面，如下图所示，单击“下一步”按钮。



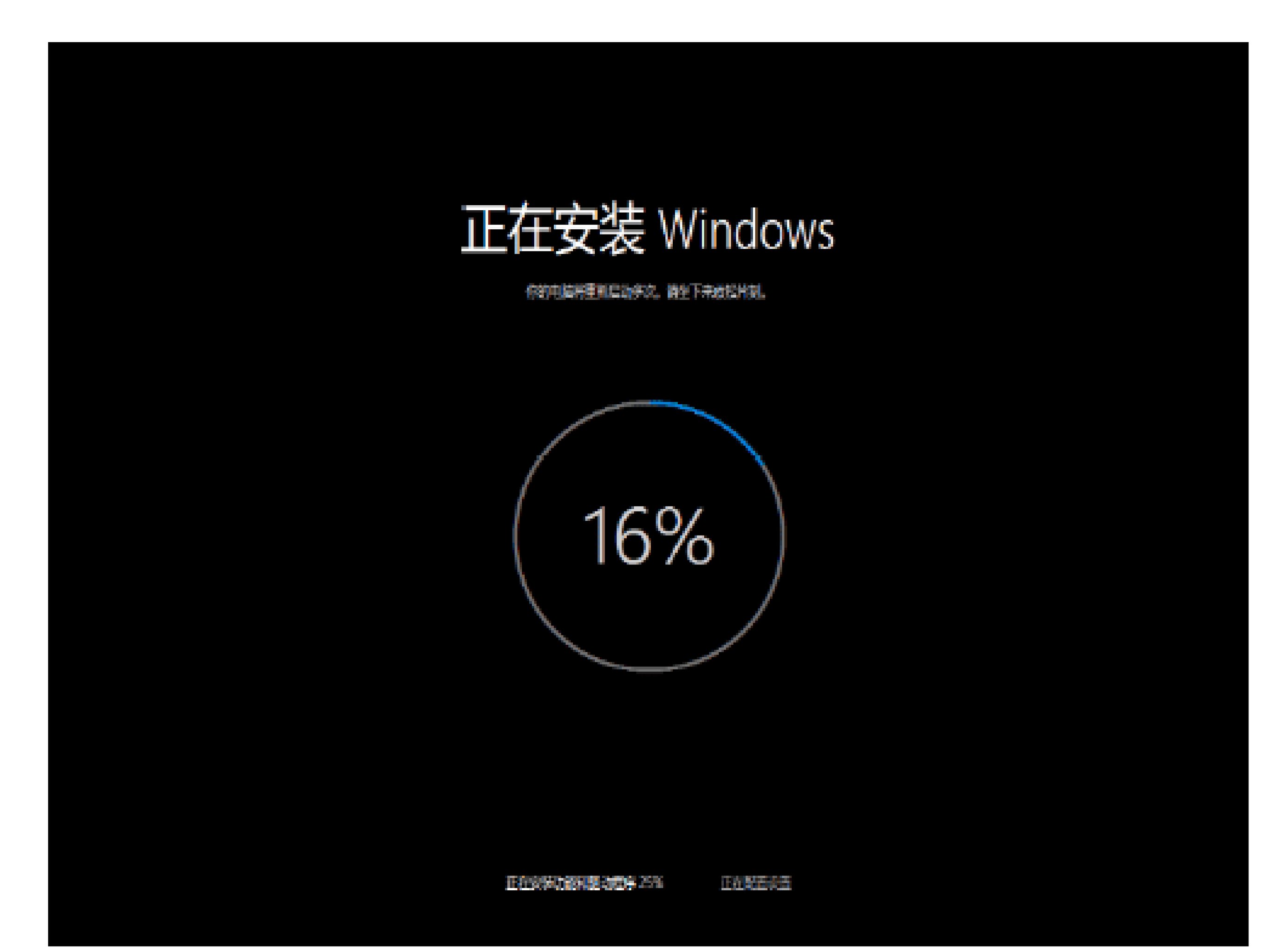
Step 06 弹出“准备就绪，可以重置这台计算机”界面，如下图所示，单击“重置”按钮。



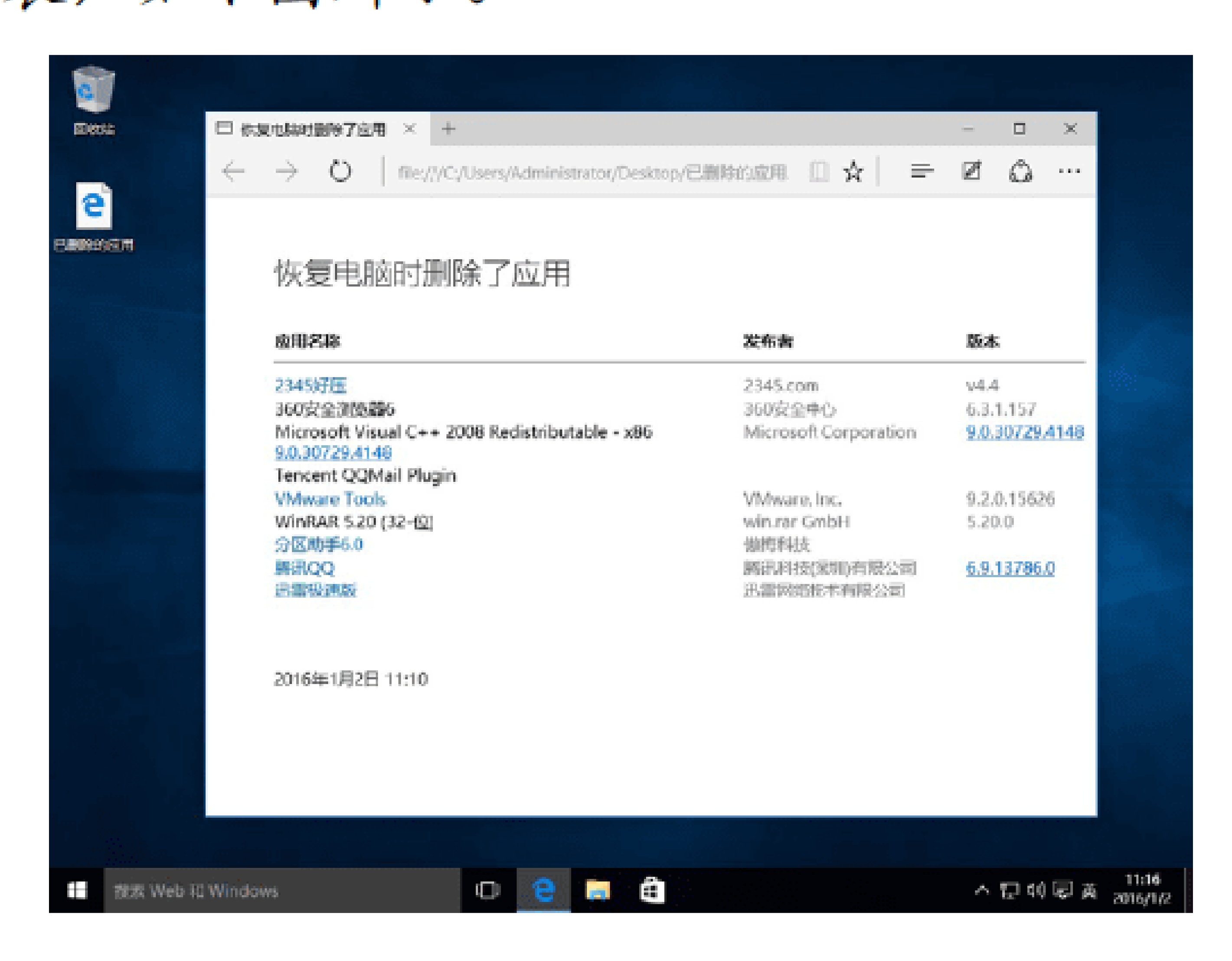
Step 07 计算机重新启动，进入“重置”界面，如下图所示。



Step 08 重置完成后，进入Windows 10安装界面，如下图所示。



Step 09 安装完成后自动进入Windows 10桌面，可以看到恢复计算机时删除的应用列表，如下图所示。



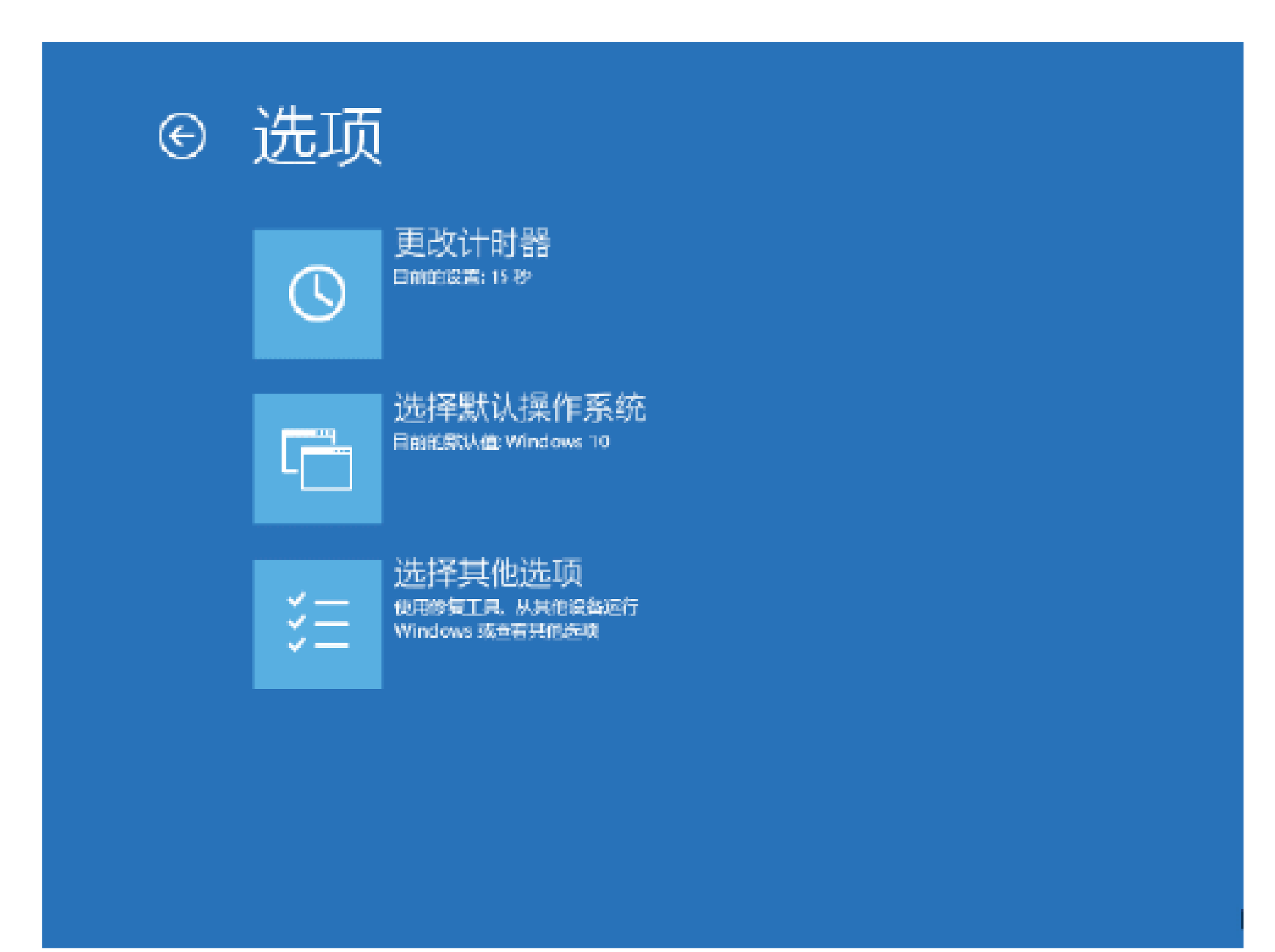
实战9：在不可开机情况下重置计算机

如果Windows 10操作系统出现错误，开机后无法进入系统，此时可以在不开机的情况下重置计算机。具体操作步骤如下。

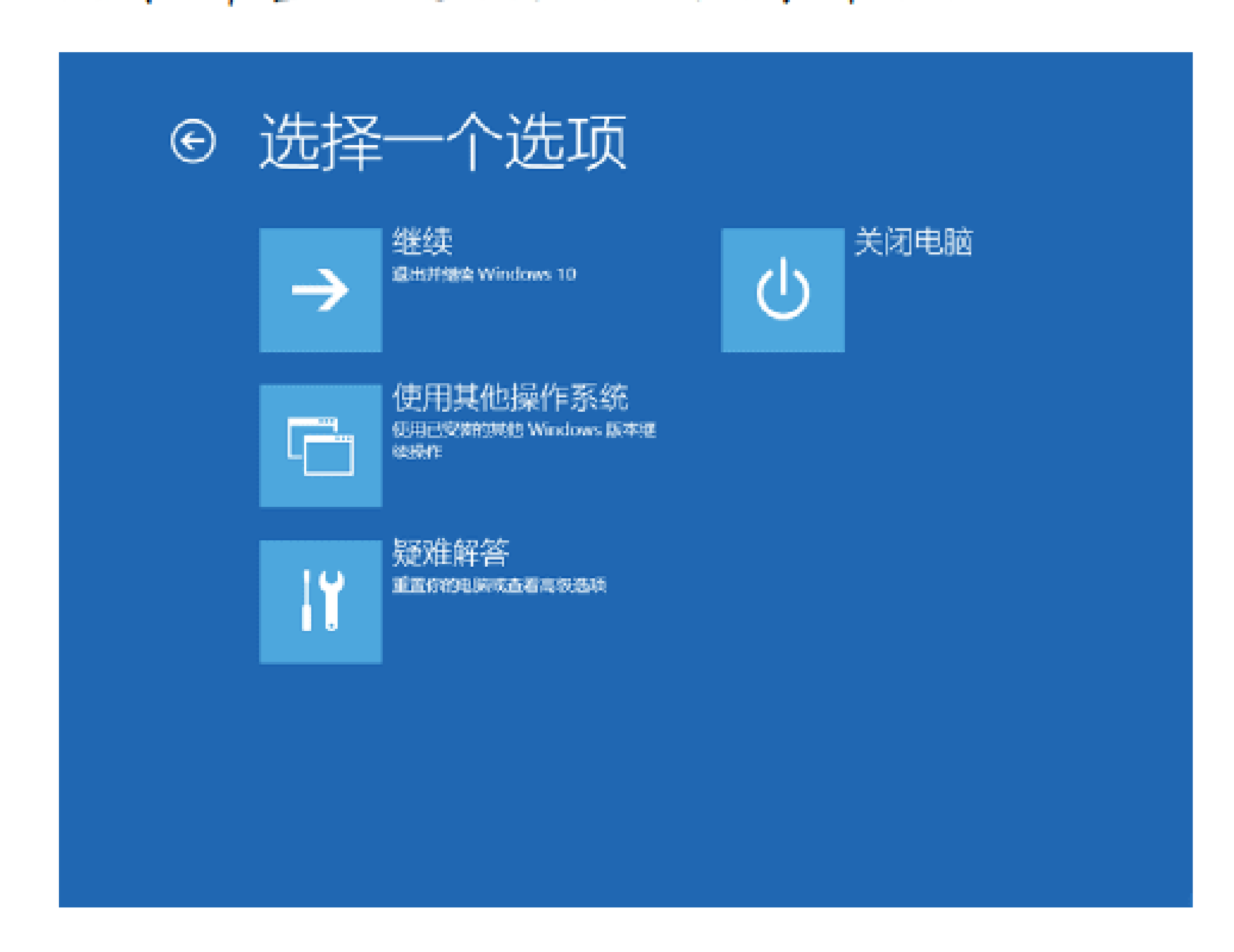
Step 01 在开机界面选择“更改默认值或选择其他选项”选项，如下图所示。



Step 02 进入“选项”界面，选择“选择其他选项”选项，如下图所示。



Step 03 进入“选择一个选项”界面，选择“疑难解答”选项，如下图所示。



Step 04 在打开的“疑难解答”界面单击“重置此计算机”选项即可，如下图所示。其后的操作与在可开机的状态下重置计算机操作相同，这里不再赘述。

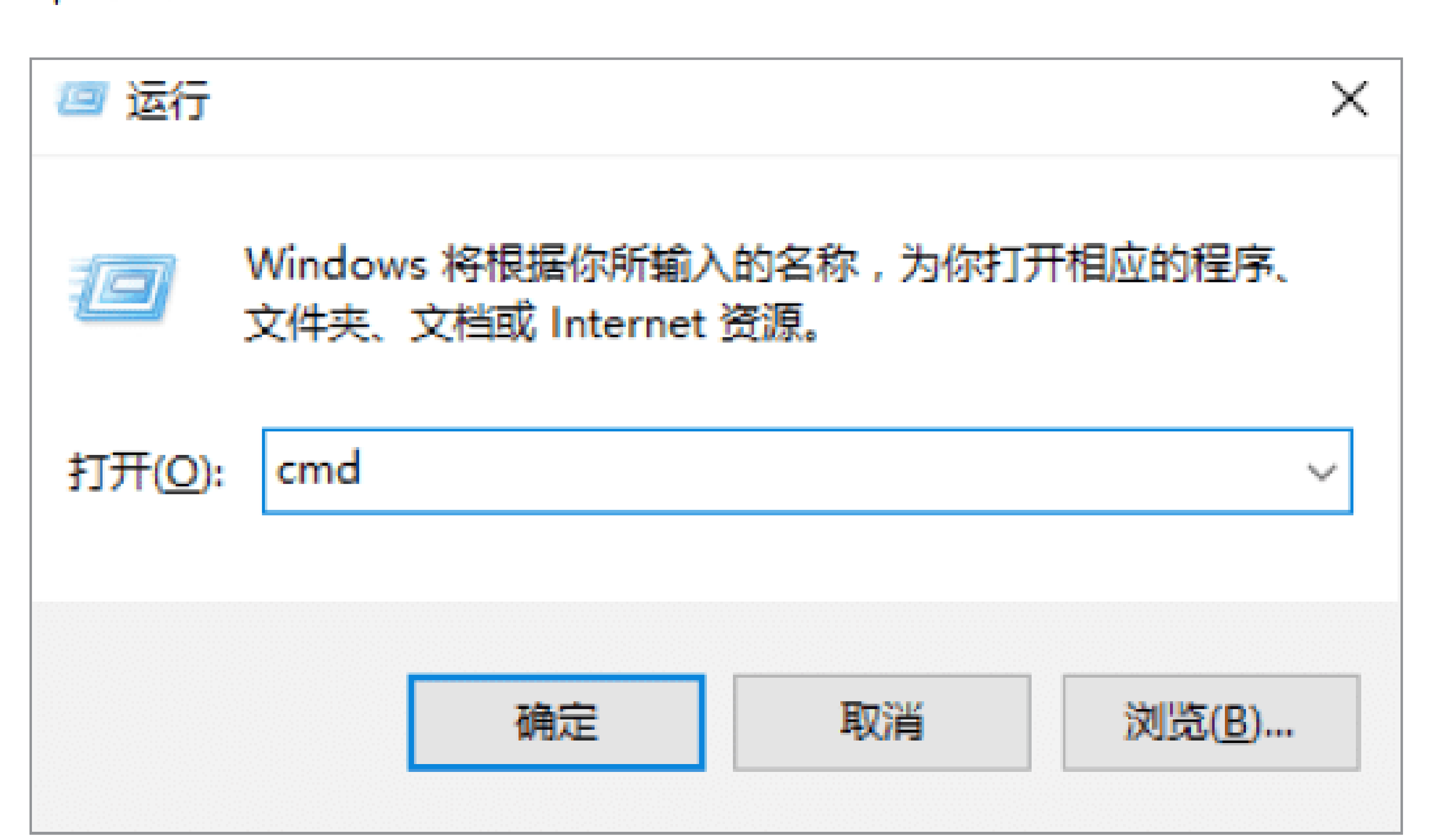


14.5　实战演练

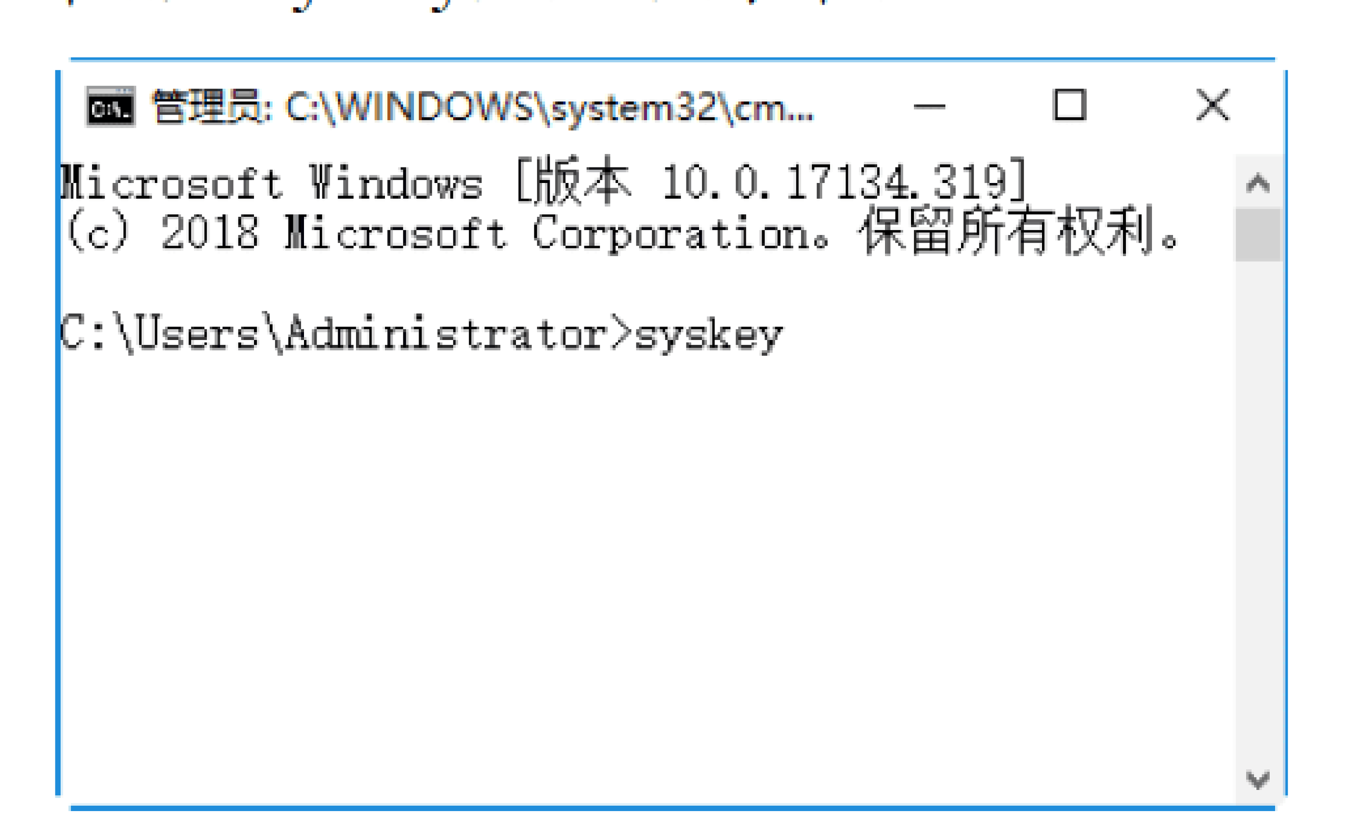
实战演练1——设置计算机系统启动密码

在Windows 10操作系统之中，用户可以设置系统启动密码。具体的操作步骤如下。

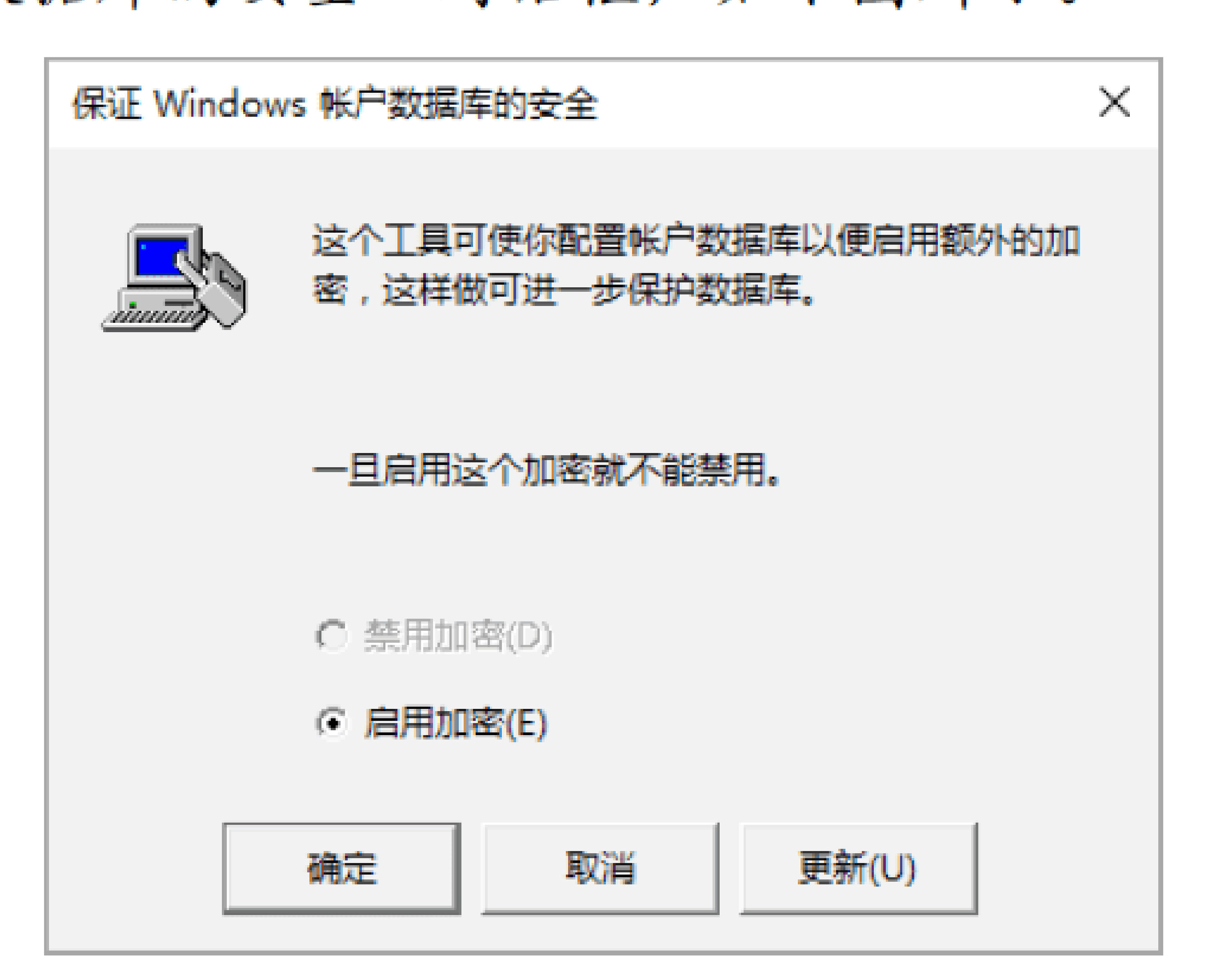
Step 01 按WIN+R组合键，打开“运行”对话框，在“打开”文本框中输入cmd，如下图所示。



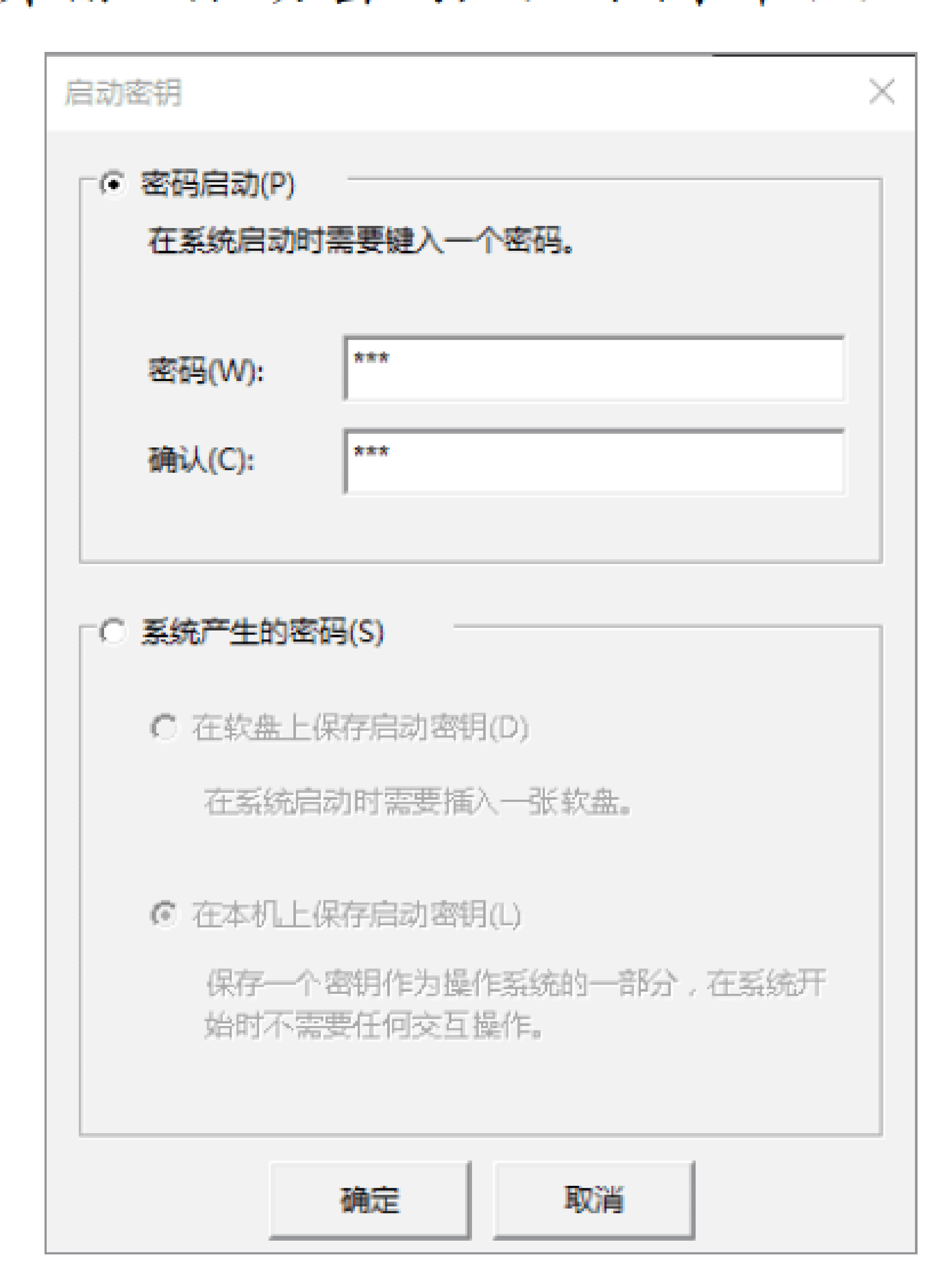
Step 02 单击“确定”按钮，在弹出的命令窗口中输入syskey，如下图所示。



Step 03 按Enter键，弹出“保证Windows账户数据库的安全”对话框，如下图所示。

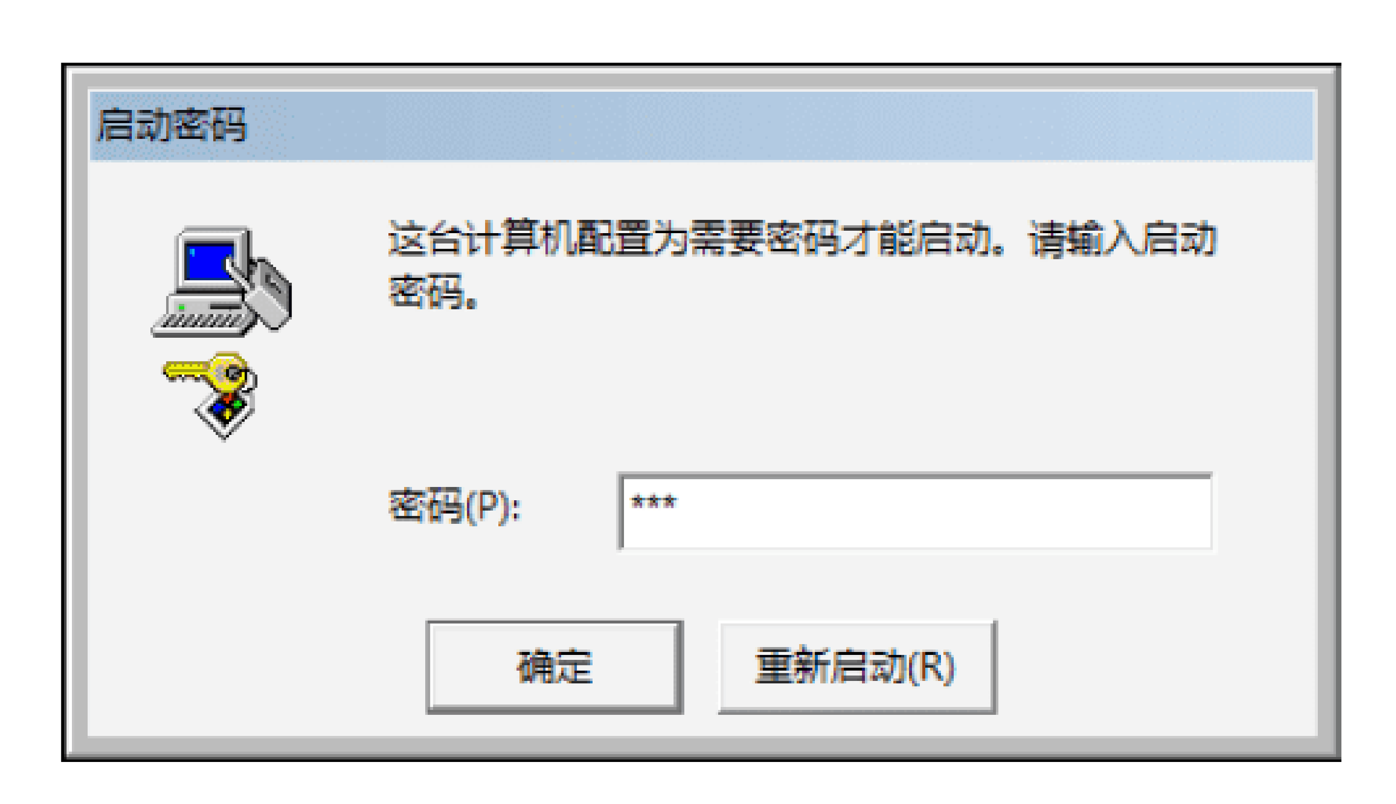


Step 04 单击“更新”按钮，弹出“启动密钥”对话框，选中“密码启动”单选按钮，并输入启动密码，如下图所示。

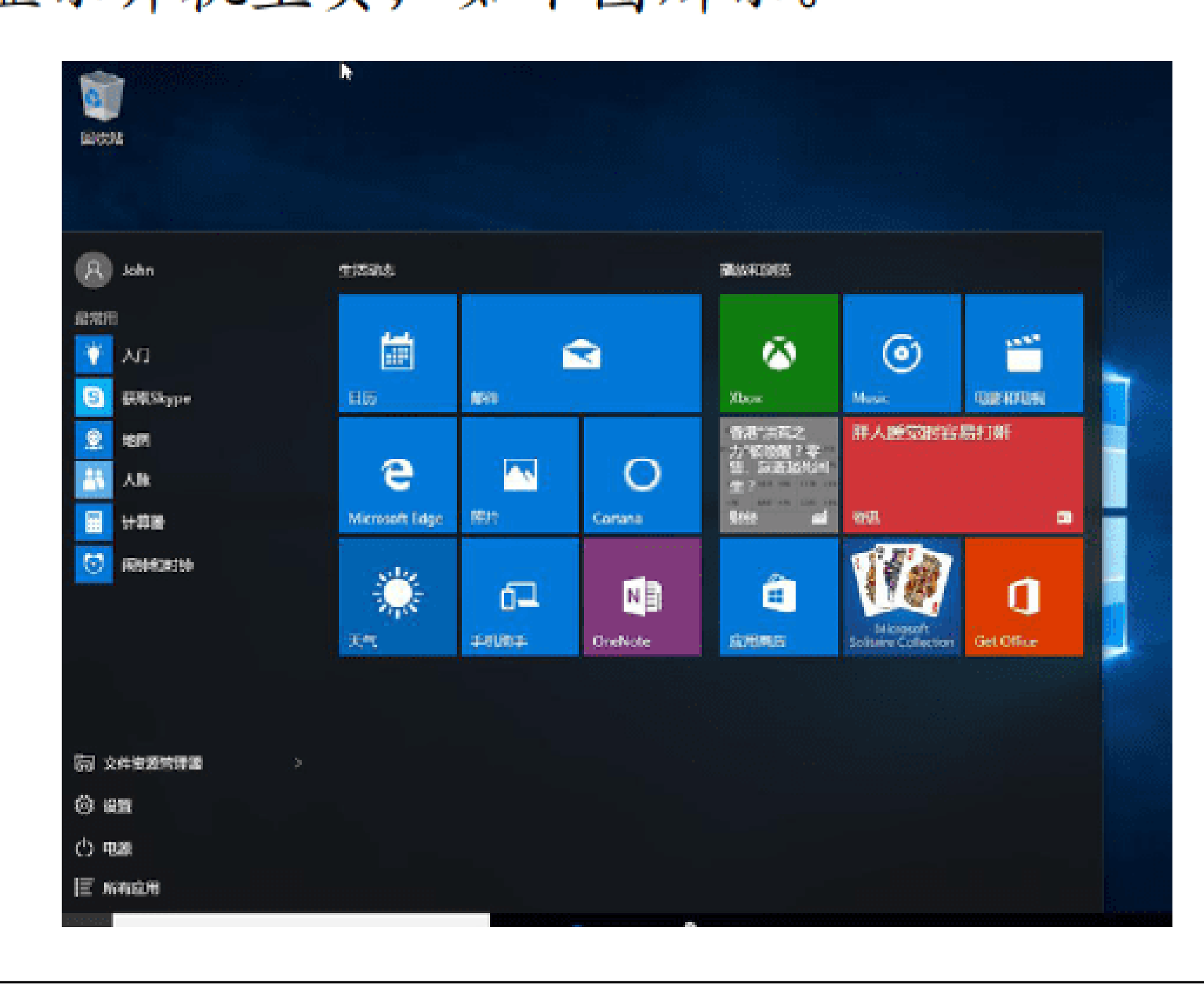


Step 05 单击“确定”按钮，重启计算机，弹出“启动密码”对话框，在其中输入密码，如下图所示。





Step 06 单击“确定”按钮，进入操作系统，显示开机主页，如下图所示。



提示：如果要取消系统启动密码，在“运行”命令窗口中输入syskey，按Enter键，在弹出的对话框中单击“更新”按钮，然后选中“系统产生的密码”和“在本机上保存启动密钥”单选按钮，单击“确定”即可，这样系统开机密码就被取消了，如下图所示。



实战演练2——创建系统修复备份光盘

使用光盘备份系统是安全又可靠的一

种方法，在进行制作系统备份光盘前需要做好以下准备。

（1）准备空白光盘。

（2）安装好操作系统带驱动的计算机。

准备工作完成后，下面就可以制作系统备份光盘了。具体的操作步骤如下。

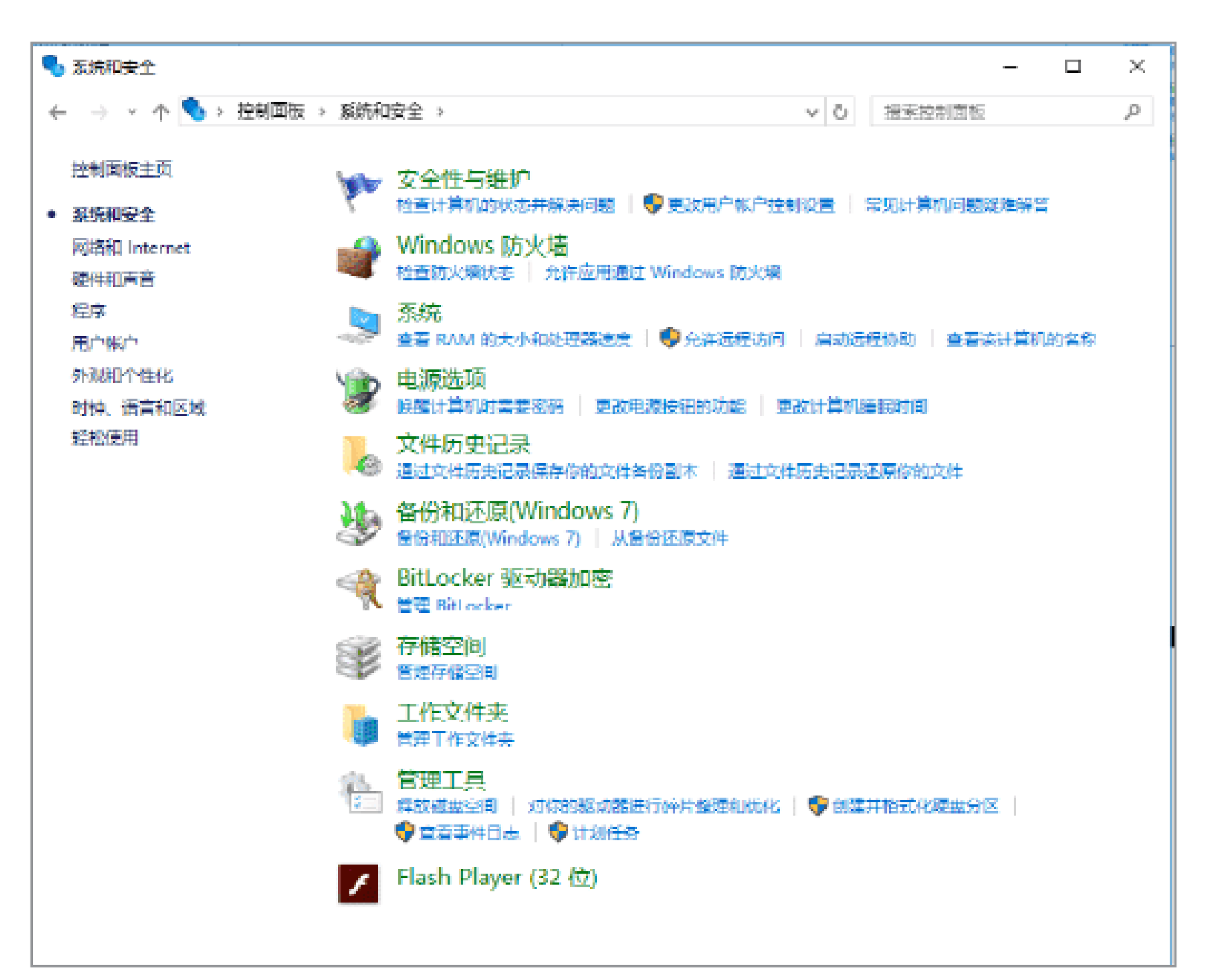
Step 01 右键单击“开始”按钮，在弹出的快捷菜单中选择“控制面板”选项，如下图所示。



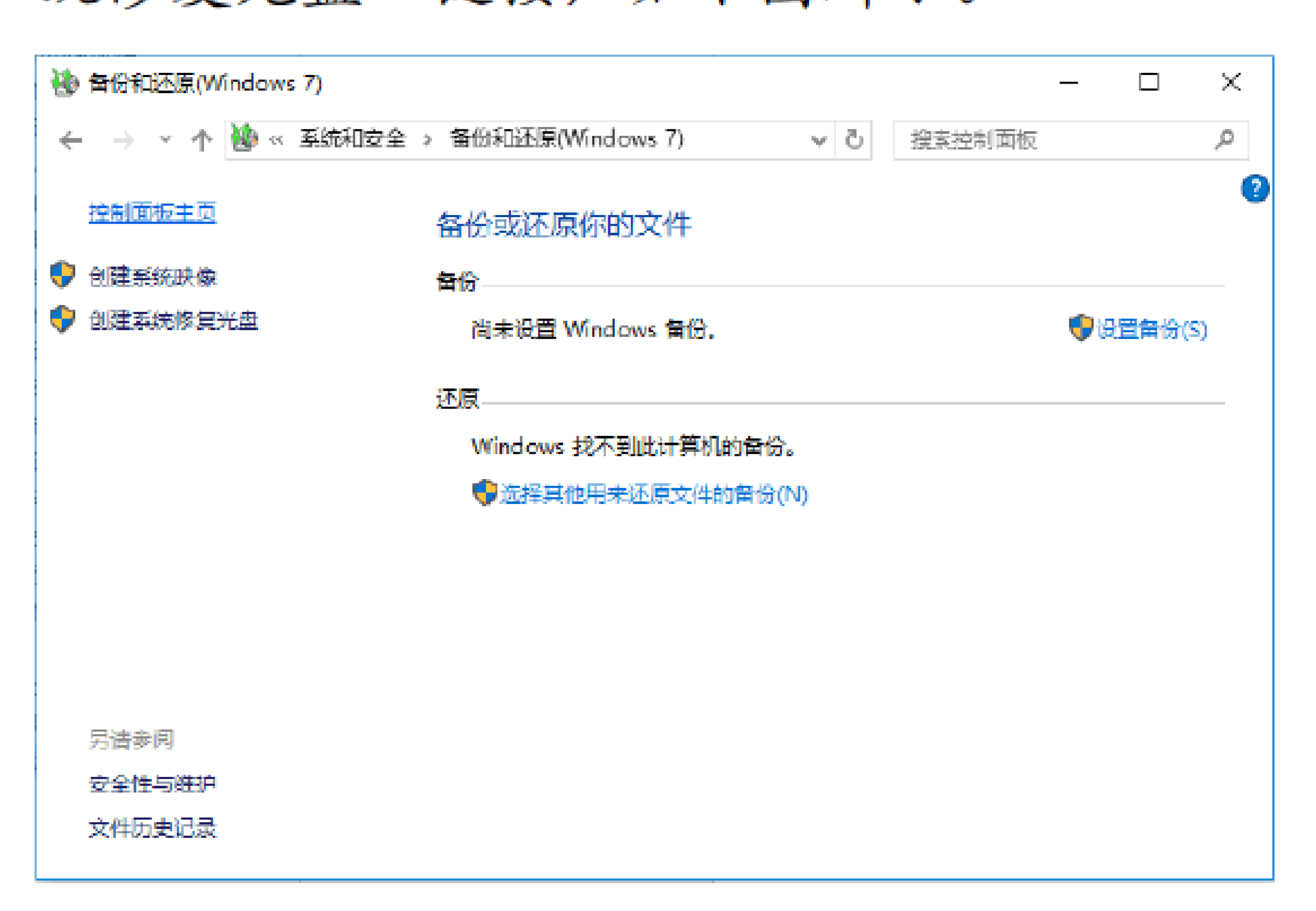
Step 02 弹出“控制面板”对话框，单击“系统和安全”链接，如下图所示。



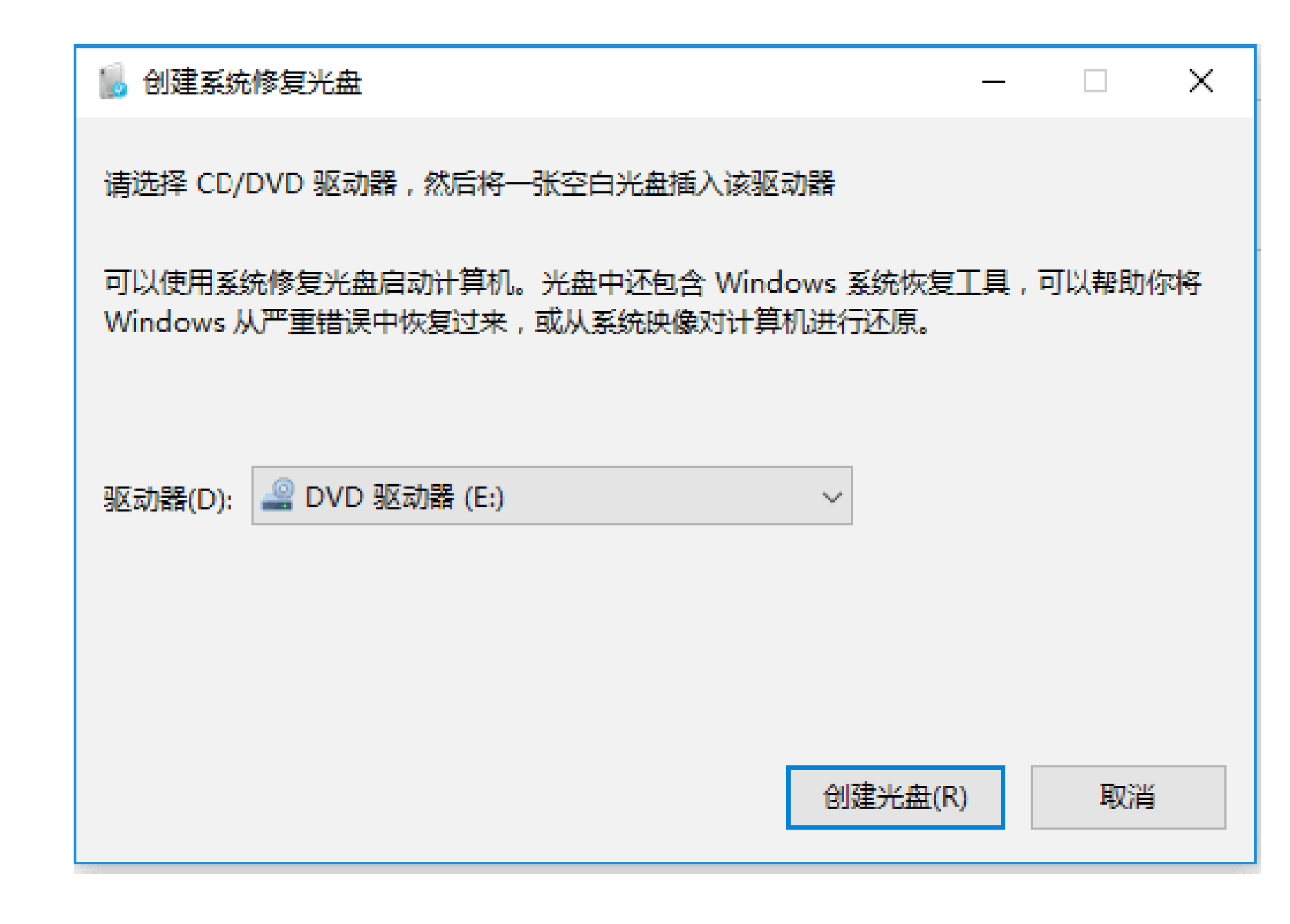
Step 03 弹出“系统和安全”对话框，单击“备份和还原”链接，如下图所示。



Step 04 打开“备份和还原”窗口，在“备份和还原”窗口的左侧窗格中单击“创建系统修复光盘”链接，如下图所示。



Step 05 弹出“创建系统修复光盘”对话框，如下图所示，在其中选择一个CD/DVD驱动器，并在此驱动器中插入空白光盘。单击“创建光盘”按钮，开始刻录系统备份光盘。



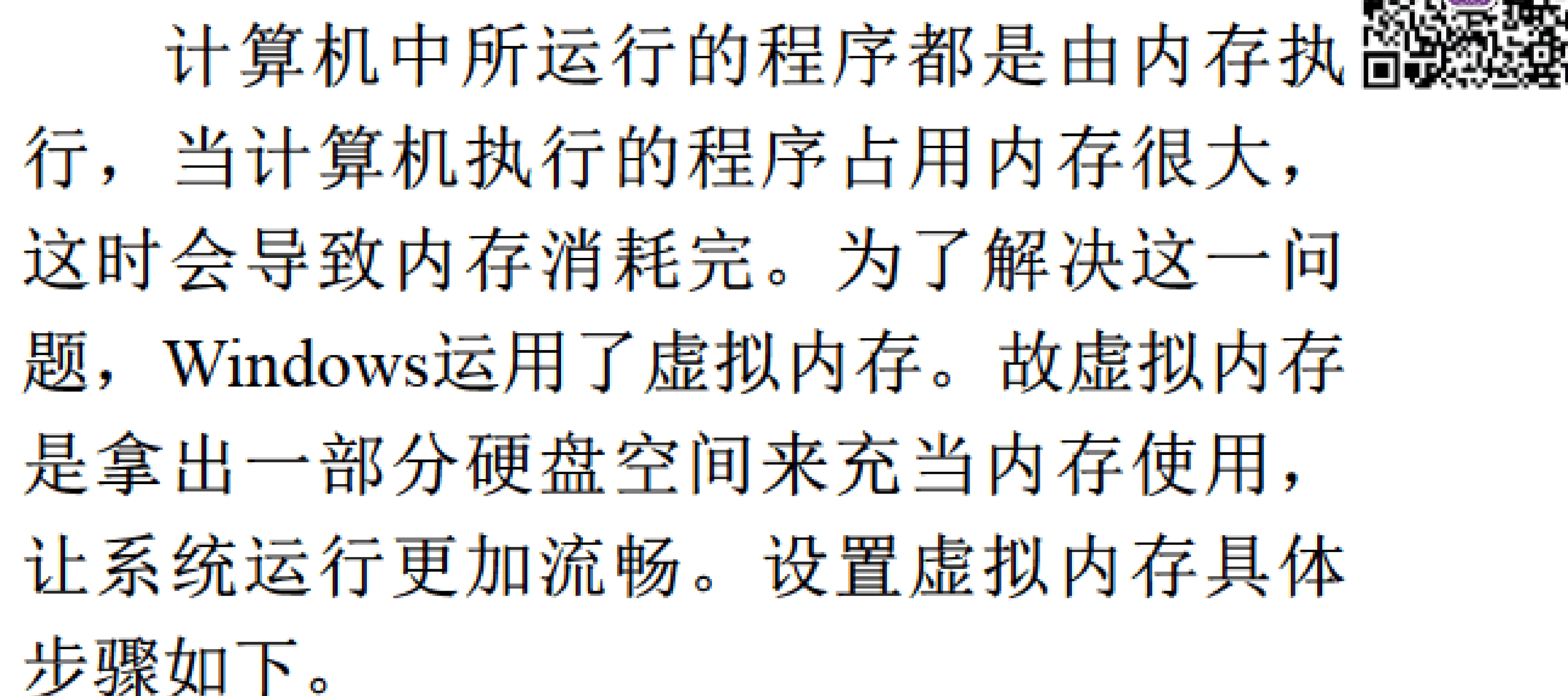
14.6 小试身手

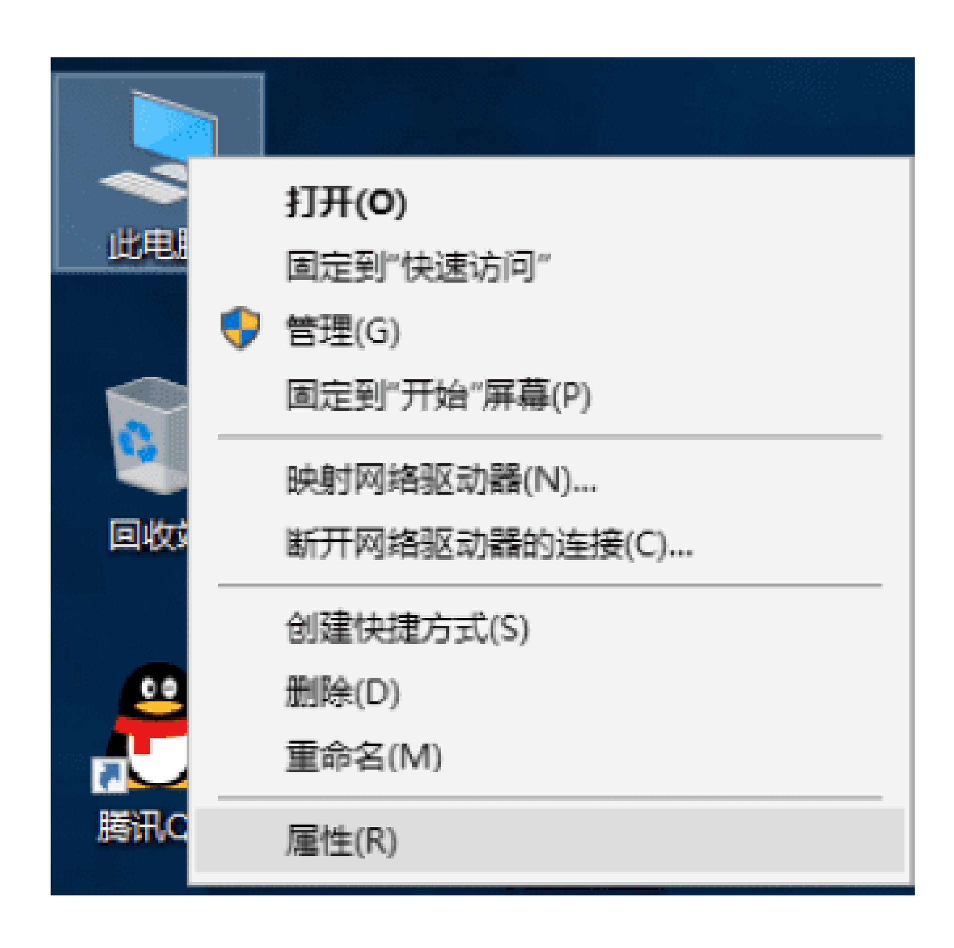
练习1：设置虚拟内存的大小



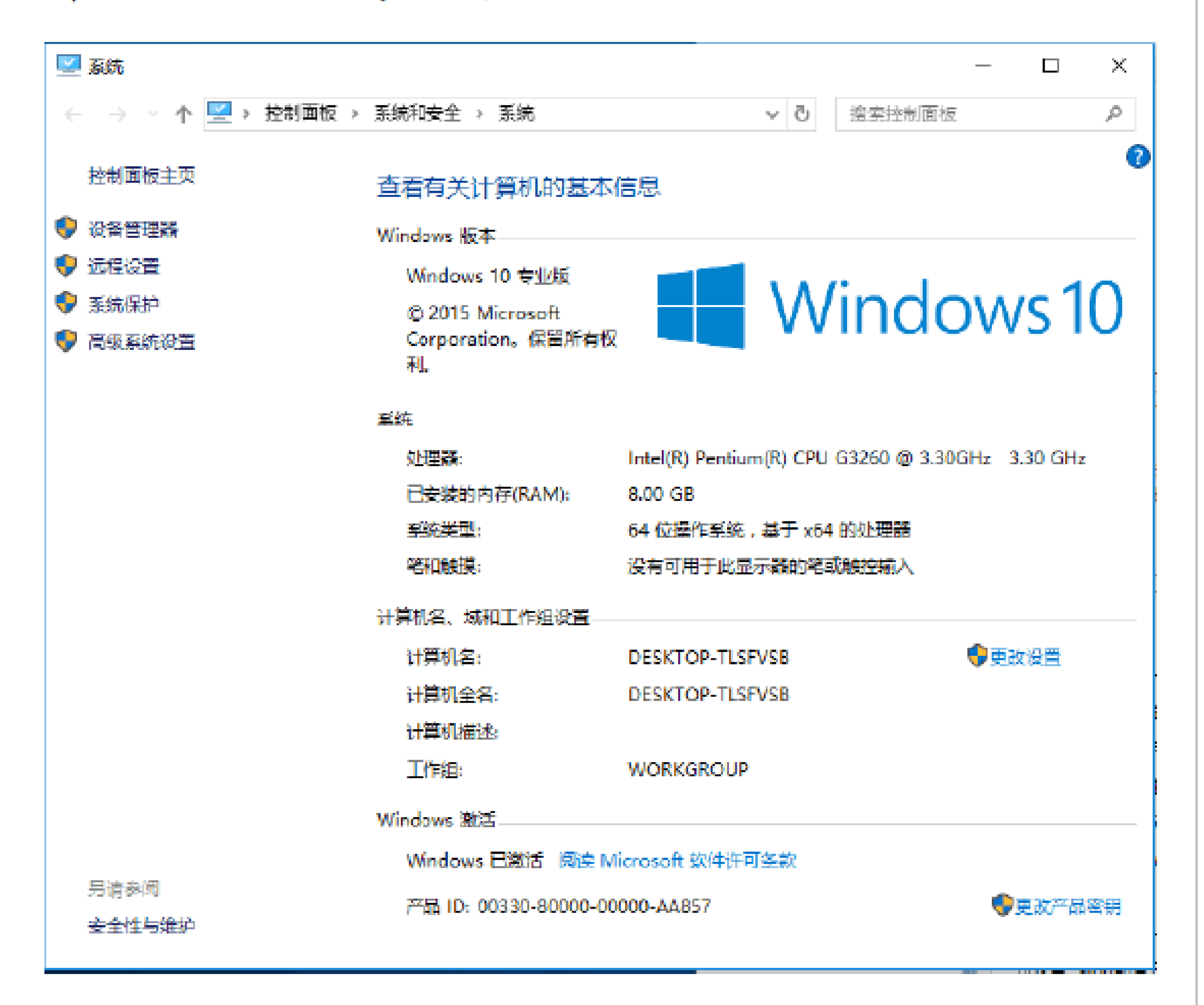
计算机中所运行的程序都是由内存执行，当计算机执行的程序占用内存很大，这时会导致内存消耗完。为了解决这一问题，Windows运用了虚拟内存。故虚拟内存是拿出一部分硬盘空间来充当内存使用，让系统运行更加流畅。设置虚拟内存具体步骤如下。

Step 01 在桌面上右键单击“此计算机”图标，在弹出的快捷菜单中选择“属性”选项，如下图所示。





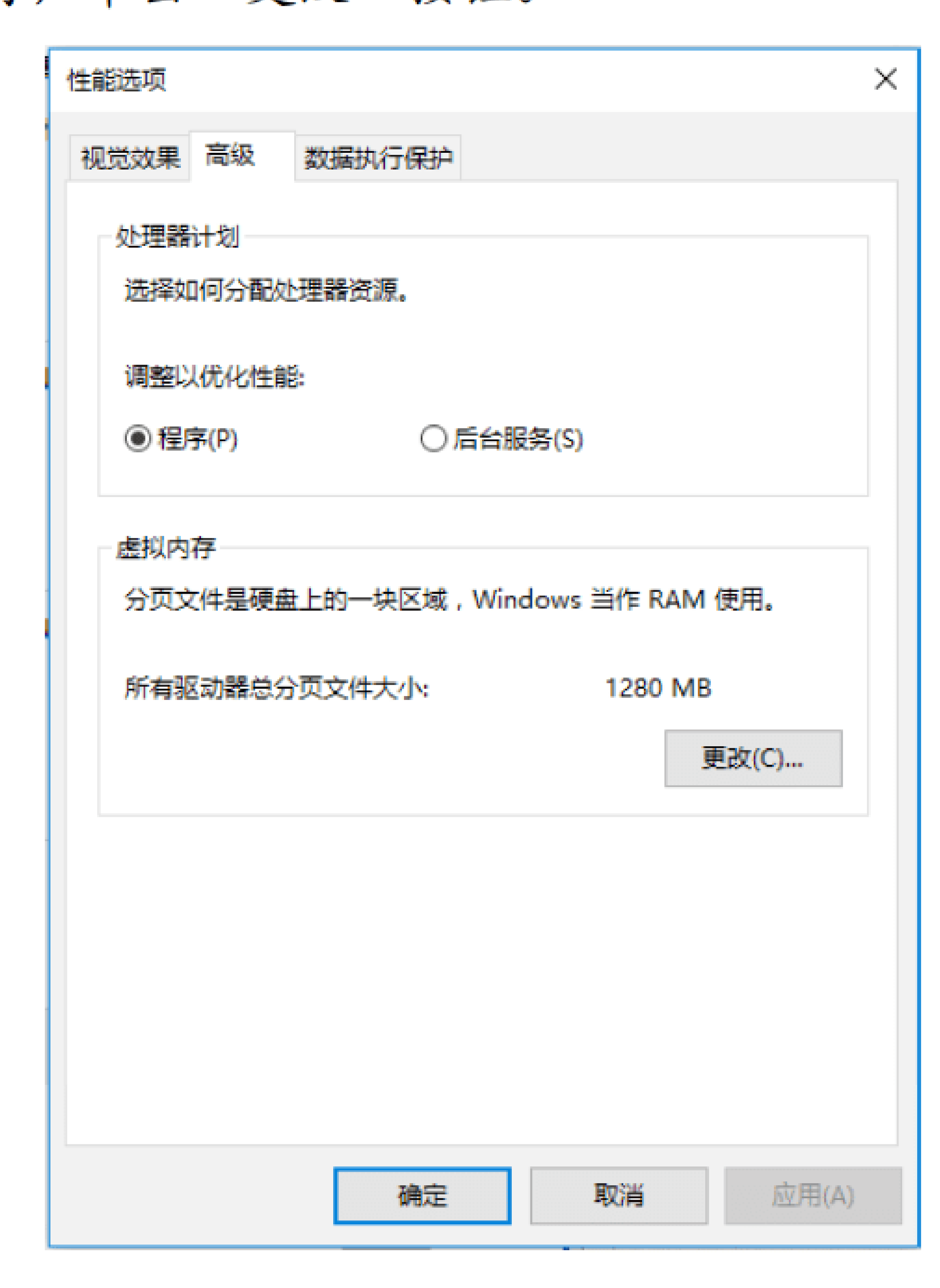
Step 02 弹出“系统”对话框，如下图所示，单击左侧“高级系统设置”链接。



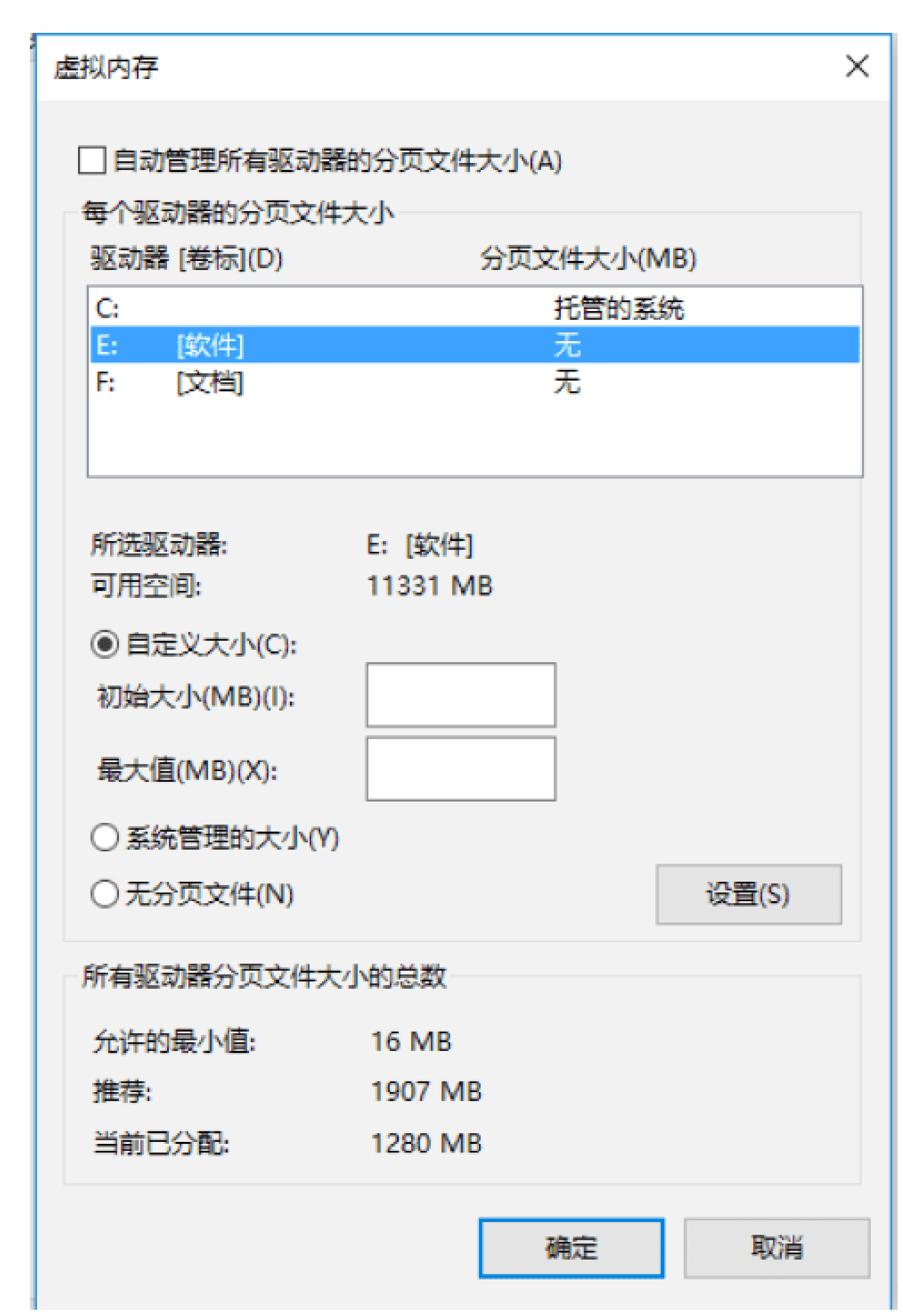
Step 03 打开“系统属性”对话框，选择“高级”选项卡，如下图所示，在其中单击“设置”按钮。



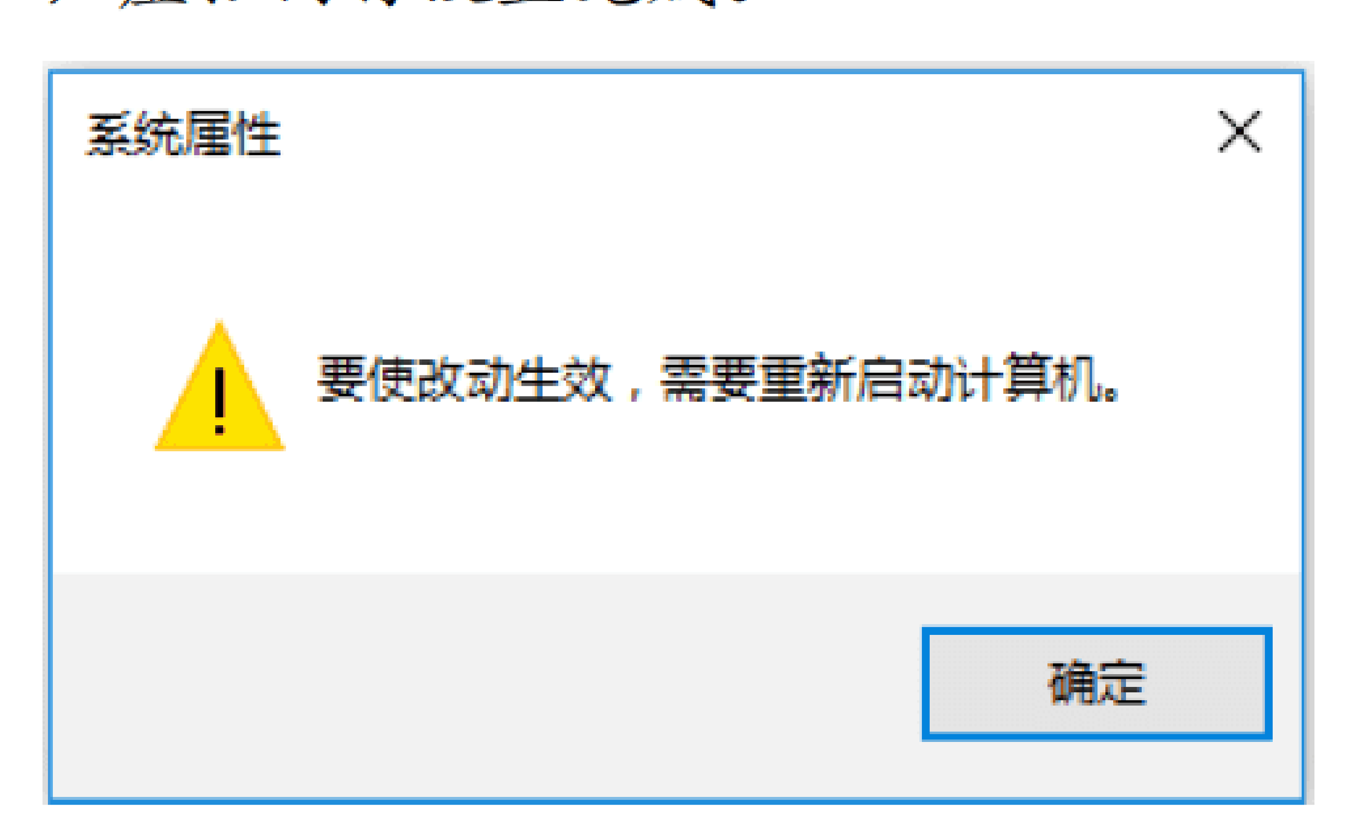
Step 04 弹出“性能选项”对话框，选择“高级”选项卡，如下图所示，设置虚拟内存，单击“更改”按钮。



Step 05 设置虚拟内存最好在非系统盘里，选中盘符，选中“自定义大小”单选按钮。输入“初始大小”和“最大值”，如下图所示，然后单击“设置”按钮。



Step 06 弹出“系统属性”提示框，如下图所示，单击“确定”按钮，重新启动计算机，虚拟内存设置完成。

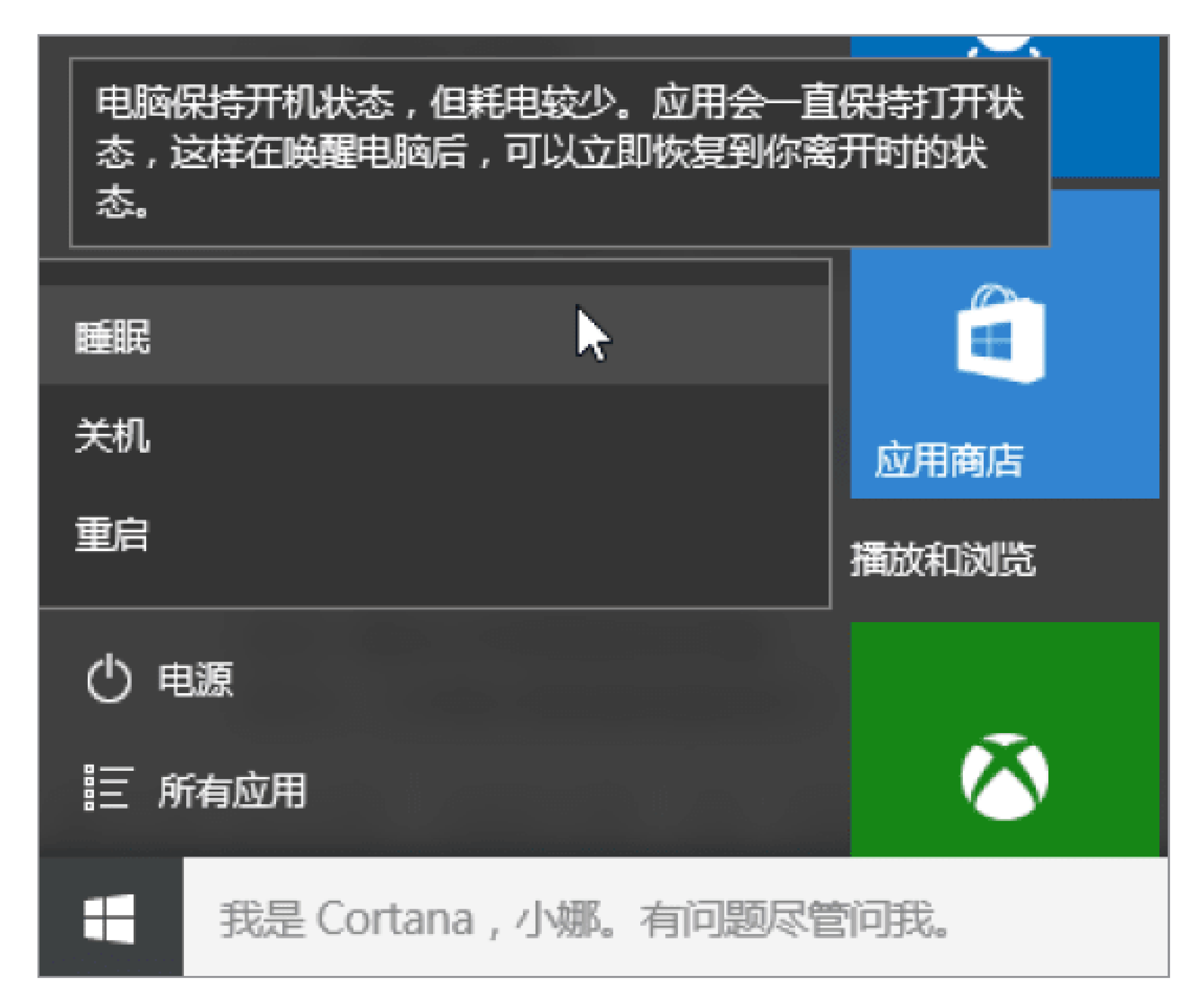


练习2：系统的睡眠与唤醒模式

在使用计算机的过程中，如果用户暂时不使用计算机，又不希望其他人在自己的计算机上任意操作时，可以将操作系统设置为睡眠模式，这样系统既能保持当前的运行，又将计算机转入低功耗状态。当用户再次使用计算机时，可以将系统唤醒。

切换系统睡眠与唤醒模式的操作步骤如下。

Step 01 单击Windows 10桌面左下角的“开始”按钮，在弹出的“开始”菜单中选择“电源”选项，在弹出的子菜单中选择“睡眠”，如下图所示。





Step 02 此时计算机进入睡眠状态，如果想唤醒计算机，双击鼠标，即可重新唤醒计算机，并进入Windows 10操作系统的锁屏桌面，然后按Enter键确认，即可进入系统桌面。下图为Windows 10操作系统的锁屏桌面。



第15章　黑客后门入侵痕迹的清理

从入侵者与远程主机/服务器建立连接起，系统就开始把入侵者的IP地址及相应操作事件记录下来，系统管理员可以通过这些日志文件找到入侵者的入侵痕迹，从而获得入侵证据及入侵者的IP地址。因此，为避免留下蛛丝马迹，入侵者在完成入侵任务之后，还要尽可能地把自己的入侵痕迹清除干净，以免被管理员发现。

15.1　黑客留下的“脚印”

日志是黑客留下的“脚印”，其本质就是对系统中的操作进行的记录，用户对计算机的操作和应用程序的运行情况都能记录下来，所以黑客在非法入侵计算机以后所有行动的过程也会被日志记录在案。

15.1.1　日志的详细定义

日志文件是Windows系统中一个比较特殊的文件，它记录着Windows系统中所发生的一切，如各种系统服务的启动、运行、关闭等信息。

日志文件通常有应用程序日志、安全日志、系统日志、DNS服务器日志和FTP日志等。当使用“流光”进行探测时，IPC（Internet Process Connection）探测会在目标机的安全日志里迅速地记下“流光”探测时所用的IP、时间等；使用FTP探测后，会在目标机的FTP日志中记下探测所用的用户名和密码等。当日志记录下这些信息后，通过日志可以轻易地找到入侵的黑客。另外，Scheduler日志，也是个重要的日志，srv.exe就是通过这个服务来启动的，其记录着由Scheduler服务启动的所有行为，如服务的启动和停止。

1）日志文件的默认位置

（1）DNS服务器日志的默认位置：%systemroot%\system32\config，默认文件大小为512KB，管理员都会改变这个默认大小。

（2）安全日志文件默认位置：%systemroot%\system32\config\SecEvent.EVT。

（3）系统日志文件默认位置：%systemroot%\system32\config\sysEvent.EVT。

（4）应用程序日志文件默认位置：%systemroot%\system32\config\AppEvent.EVT。

（5）Internet信息服务FTP日志默认位置：%systemroot%\system32\logfiles\msftpsvc1\，默认每天一个日志。

（6）Internet信息服务WWW日志默认位置：%systemroot%\system32\logfiles\w3svc1\，默认每天一个日志。

（7）Scheduler服务日志默认位置：%systemroot%\schedlgu.txt。

2）日志在注册表里的键

（1）应用程序日志、安全日志、系统日志、DNS服务器日志的文件在注册表中的键为HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\Eventlog，有的管理员很可能将这些日志重定位。其中Eventlog下面有很多子表，里面可查看到以上日志的定位目录。

（2）Schedluler服务日志在注册表中的键为HKEY_LOCAL_MACHINE\SOFTWARE\ Microsoft\SchedulingAgent。

3）FTP日志和WWW日志

FTP日志和WWW日志在默认情况下，每天生成一个日志文件，包括当天的所有记录。文件名通常为ex年份月份日期，例如ex001023就是2000年10月23日产生的日

志文件。从日志里能看出黑客入侵时间、使用的IP地址以及探测时使用的用户名，这样使得管理员可以想出相应的对策。

15.1.2　为什么要清理日志

Windows网络操作系统都设计有各种各样的日志文件，如应用程序日志、安全日志、系统日志、Scheduler服务日志、FTP日志、WWW日志、DNS服务器日志等，这些根据用户系统开启的服务的不同而有所不同。当在系统上进行一些操作时，这些日志文件通常会记录用户操作的一些相关内容，这些内容对系统安全工作人员相当有用。比如说有人对系统进行了IPC探测，系统就会在安全日志里迅速地记录探测者探测时所用的IP、时间、用户名等，用FTP探测后，就会在FTP日志中记录IP、时间、探测所用的用户名等。

在Windows系统中，日志文件通常有应用程序日志、安全日志、系统日志、DNS服务器日志、FTP日志、WWW日志等，其文件名为log.txt。

黑客们在获得服务器的系统管理员权限之后，就可以随意破坏系统上的文件了，包括日志文件。但是这一切都将被系统日志所记录下来，所以黑客们想要隐藏自己的入侵踪迹，就必须对日志进行修改。最简单的方法就是删除系统日志文件，但这样做一般都是初级黑客所为，真正的高级黑客们总是用修改日志的方法来防止系统管理员追踪到自己，网络上有很多专门进行此类功能的程序，如Zap、Wipe等。

当前的计算机病毒越来越复杂，对于网上求助这种远程的判断和分析来说，必须借助第三方的软件分析，借助日志文件的内容，高手们能够分析出用户系统的大部分故障以及IE浏览器被劫持、恶意插件、流氓软件以及部分的木马病毒等。

为了防止管理员发现计算机被黑客入侵后，通过日志文件查到黑客的来源，入侵者都会在断开与入侵的主机连接前删除入侵时的日志。

15.2　分析系统日志信息

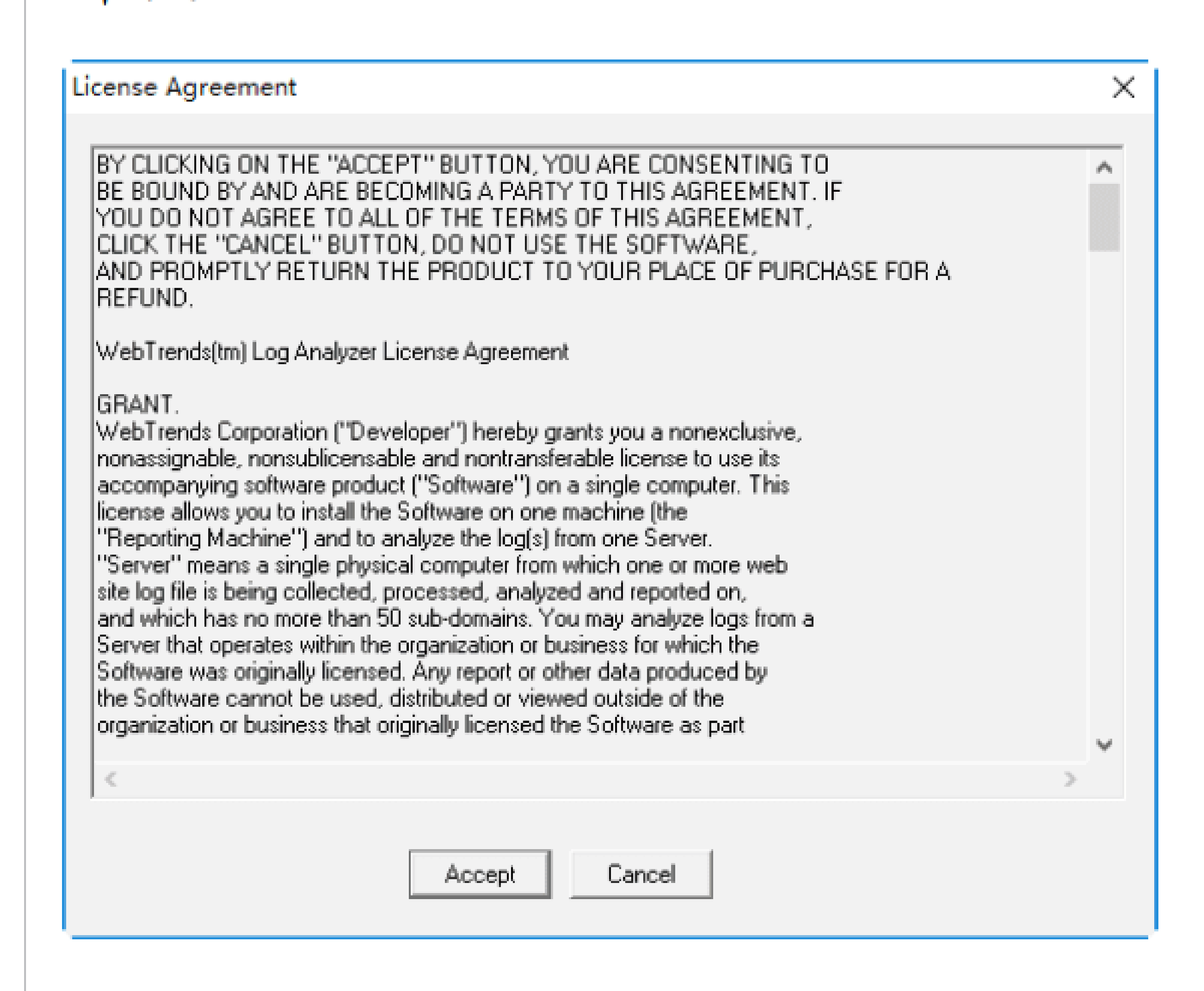
作为一名入侵者，在清理入侵记录和痕迹之前，最好是先分析一个入侵日志，从中找出需要保留的入侵信息和记录。WebTrends是一款非常好的日志分析软件，它可以很方便地生成日报、周报和月报等，并有多种图表生成方式，如柱状图、曲线图、饼图等。

实战1：安装WebTrends日志分析工具

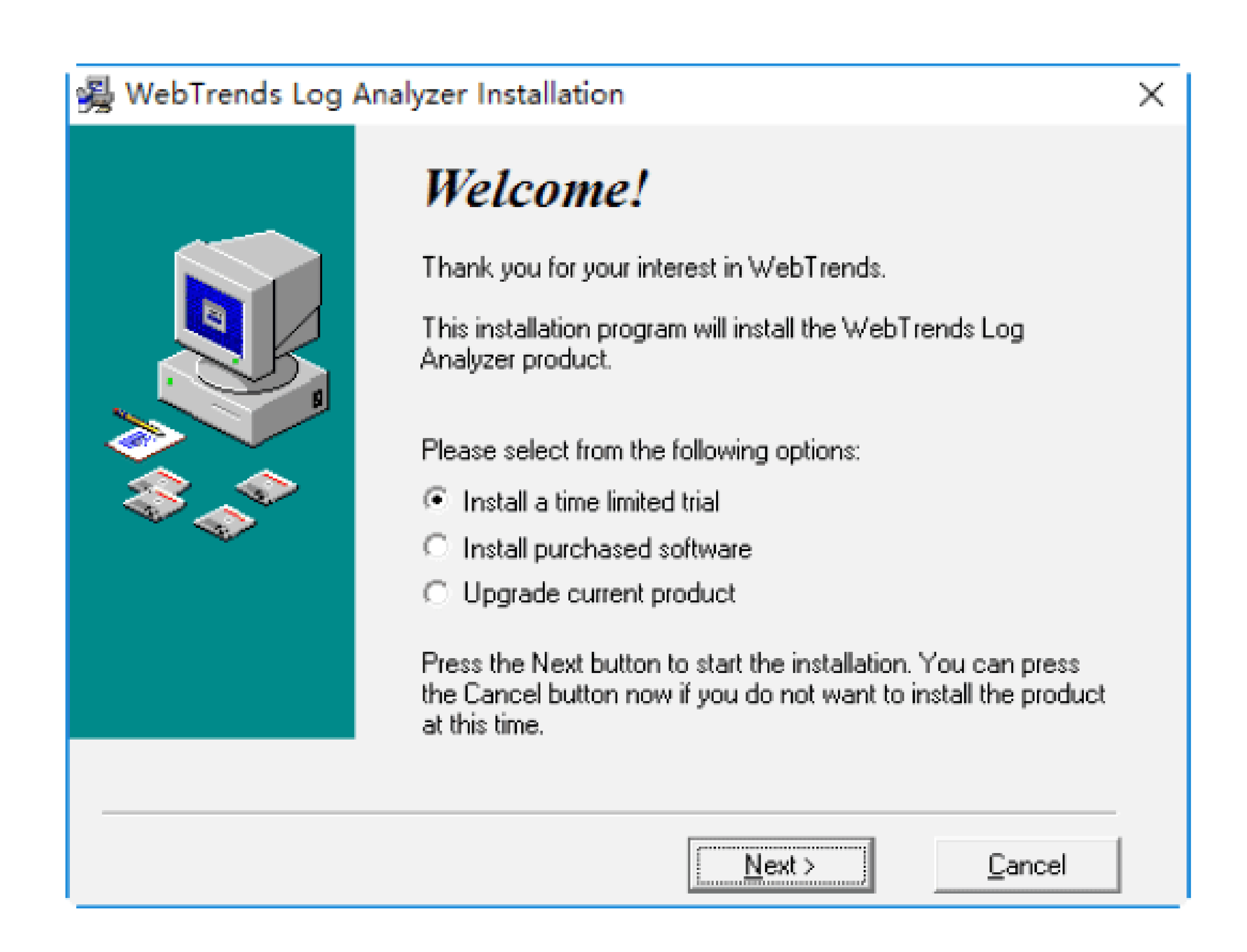


在使用之前先安装WebTrends软件，具体的操作步骤如下。

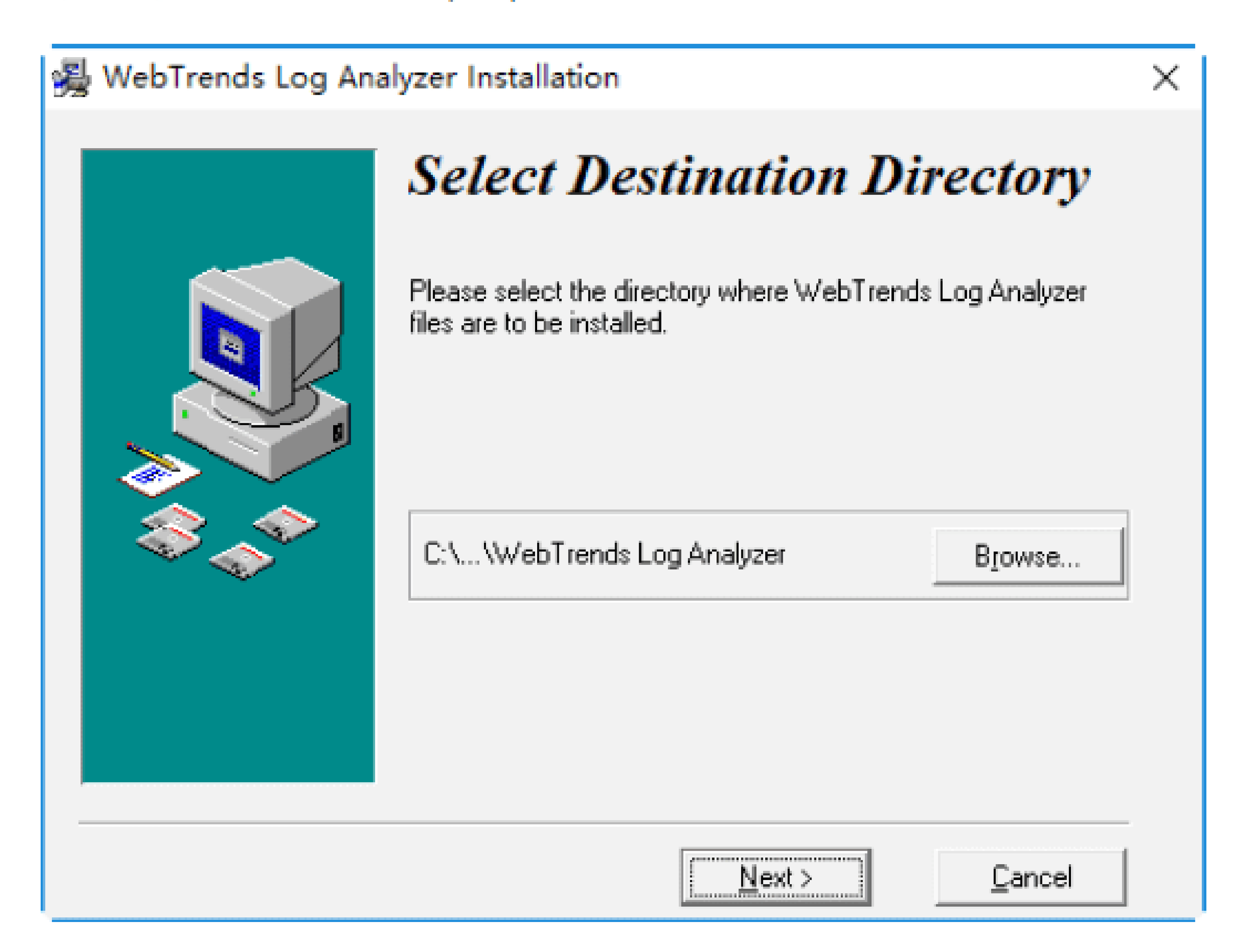
Step 01 下载并双击WebTrends安装程序图标，打开License Agreement对话框，如下图所示。



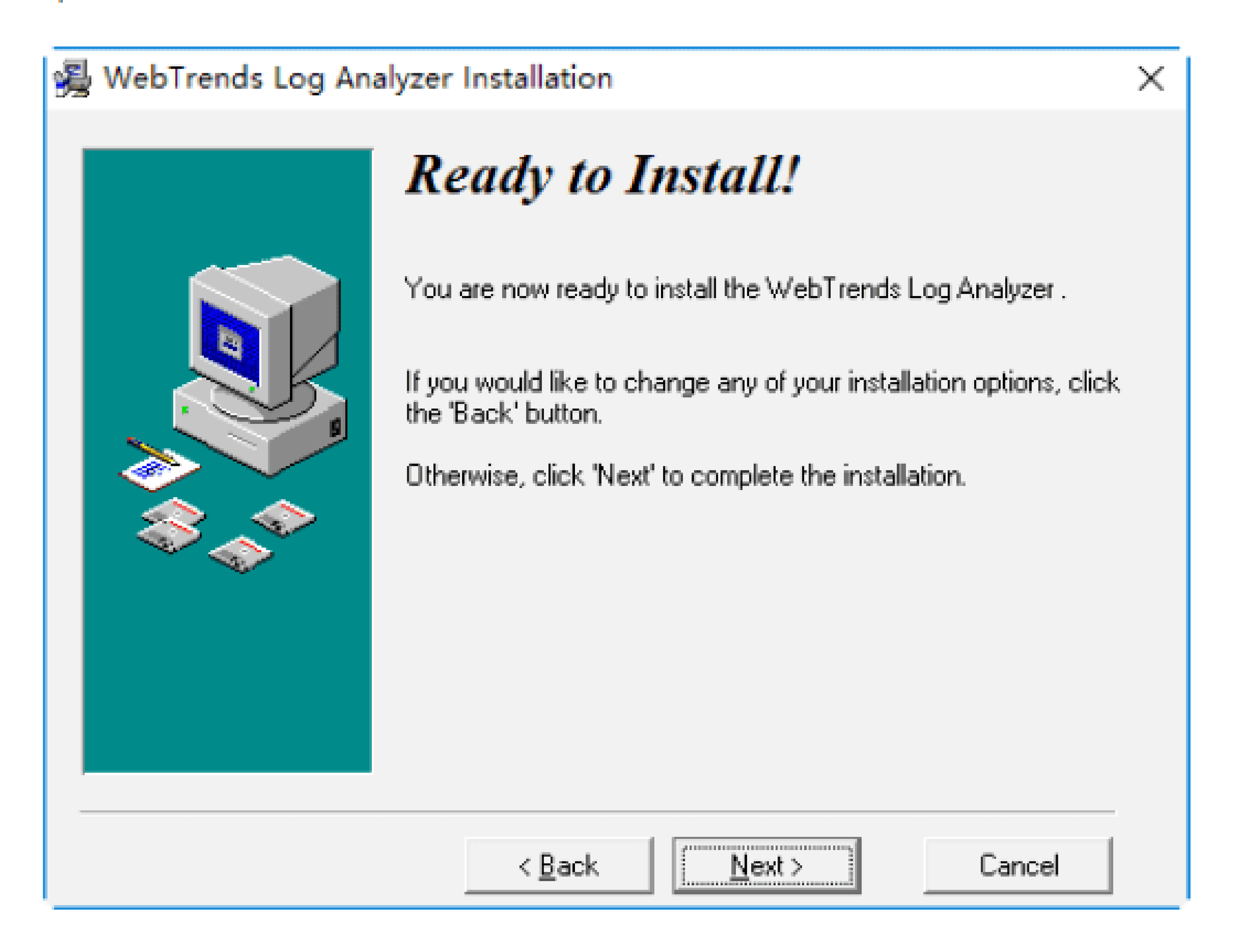
Step 02 在认真阅读安装许可协议后，单击Accept按钮，即可进入Welcome!对话框，在Please select from the following options中选中Install a time limited trial单选按钮，如下图所示。



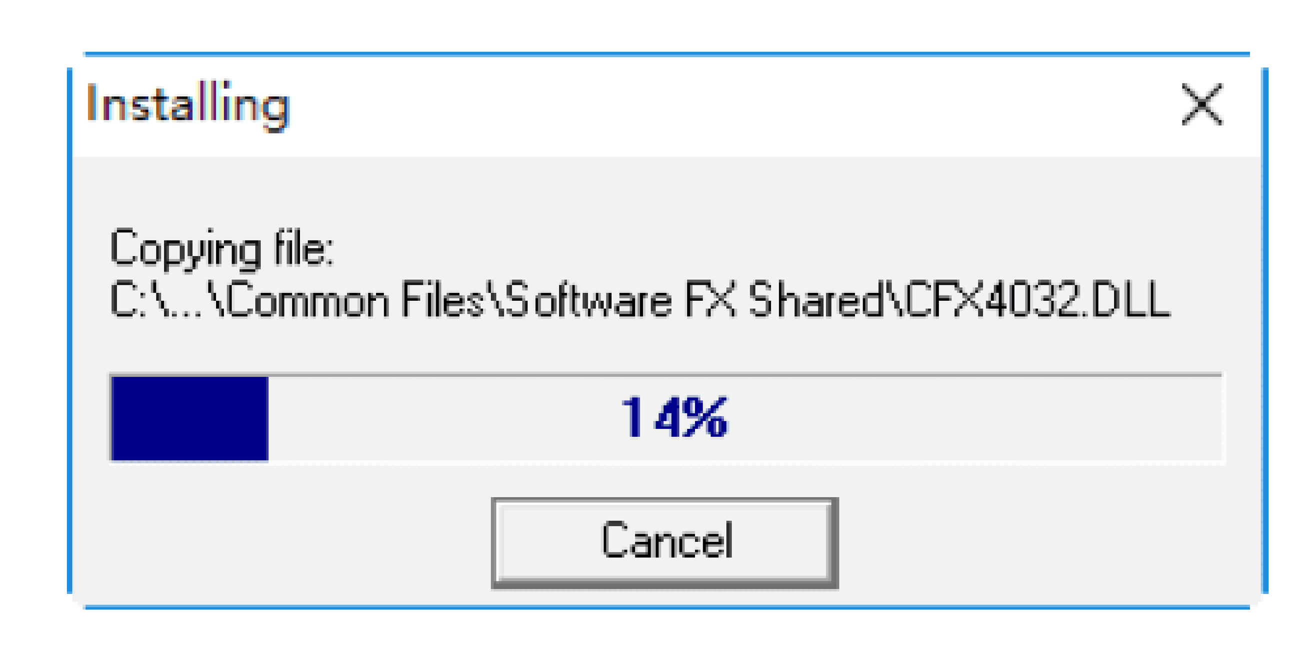
Step 03 单击Next按钮，打开Select Destination Directory对话框，在其中选择目标程序安装的位置，如下图所示。



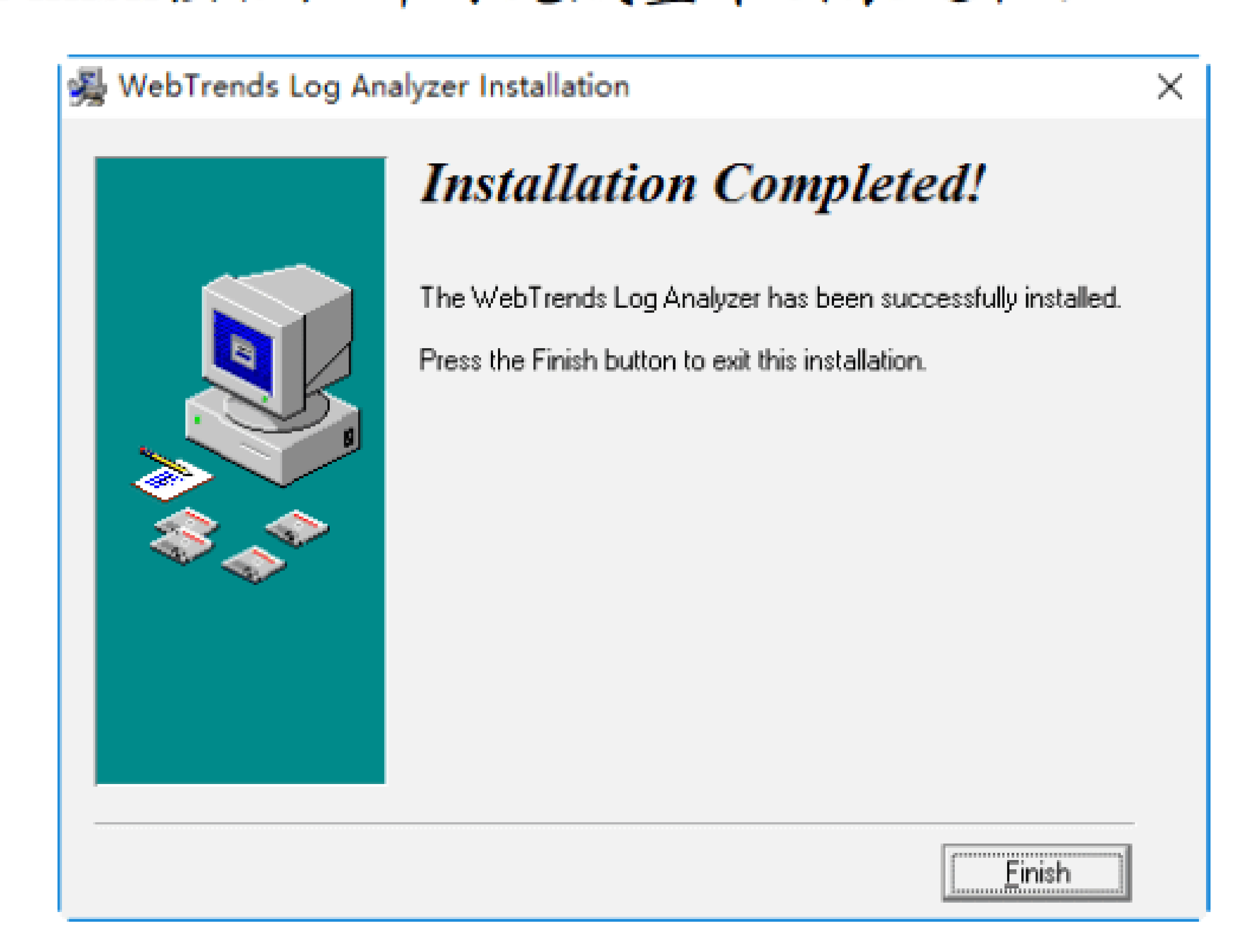
Step 04 在选择好需要安装的位置之后，单击Next按钮，打开Ready to Install！对话框，在其中可以看到安装复制的信息，如下图所示。



Step 05 单击Next按钮，打开Installing对话框，在其中看到安装的状态并显示安装进度条，如下图所示。



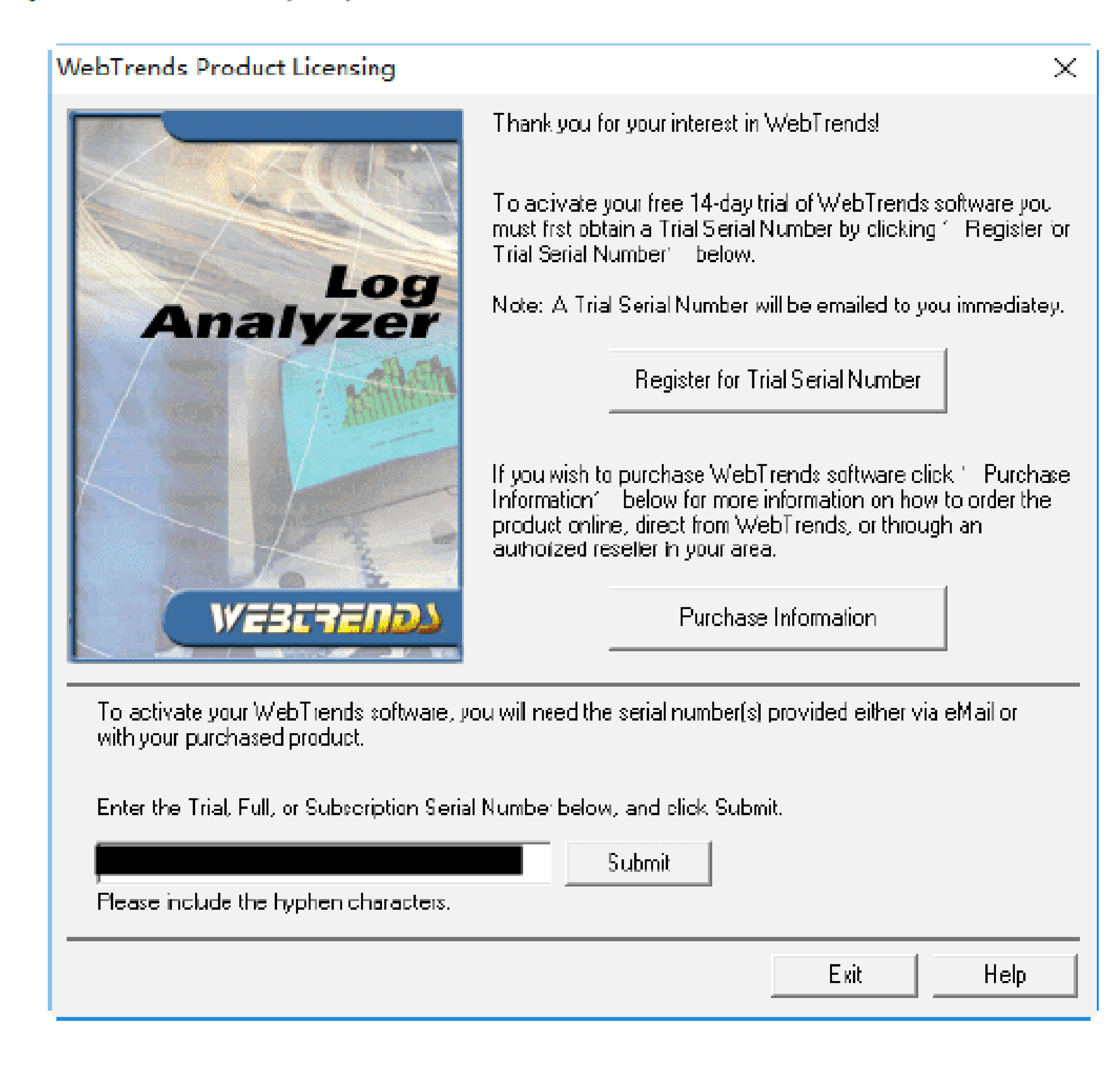
Step 06 安装完成之后，打开Installation Completed!对话框，如下图所示，单击Finish按钮，即可完成整个安装过程。



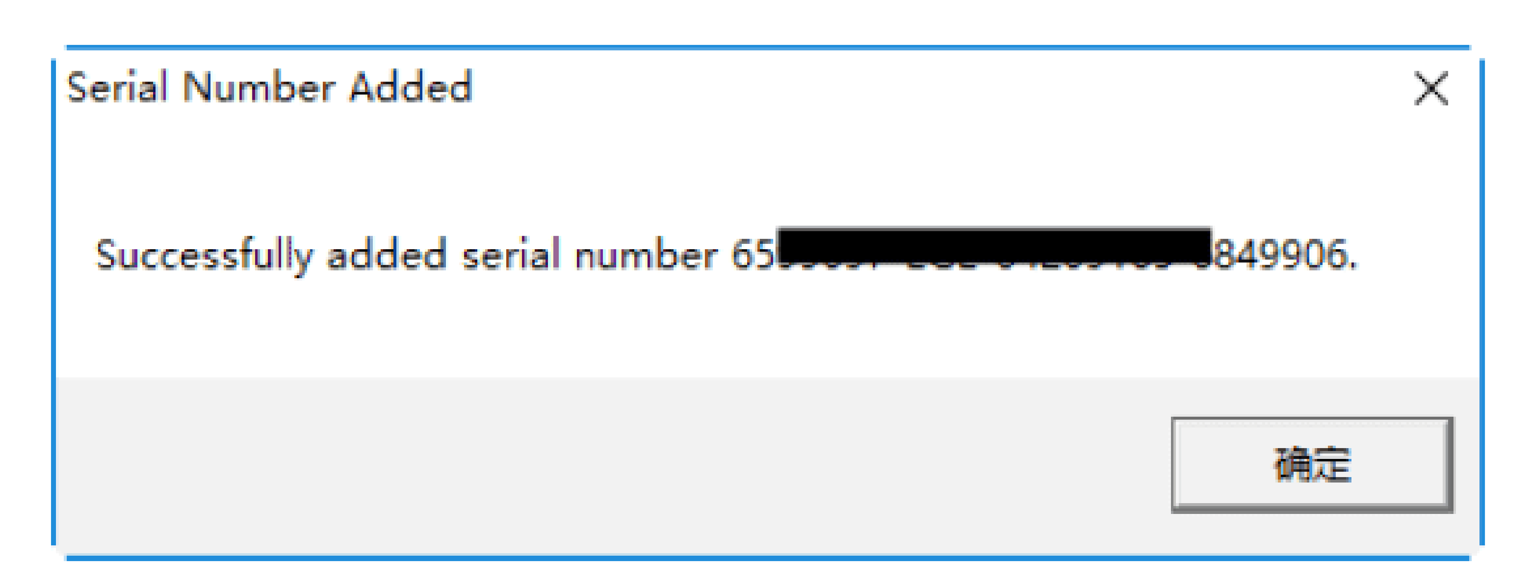
实战2：在WebTrends中创建日志站点

在WebTrends使用之前，用户必须先建立一个新的站点，在WebTrends中创建日志站点的具体操作步骤如下。

Step 01 在安装WebTrends完成之后，选择“开始”→“所有程序”→WebTrends LogAnalyzer 6.5选项，打开WebTrends Product Licensing对话框，在其中输入序列号，如下图所示。



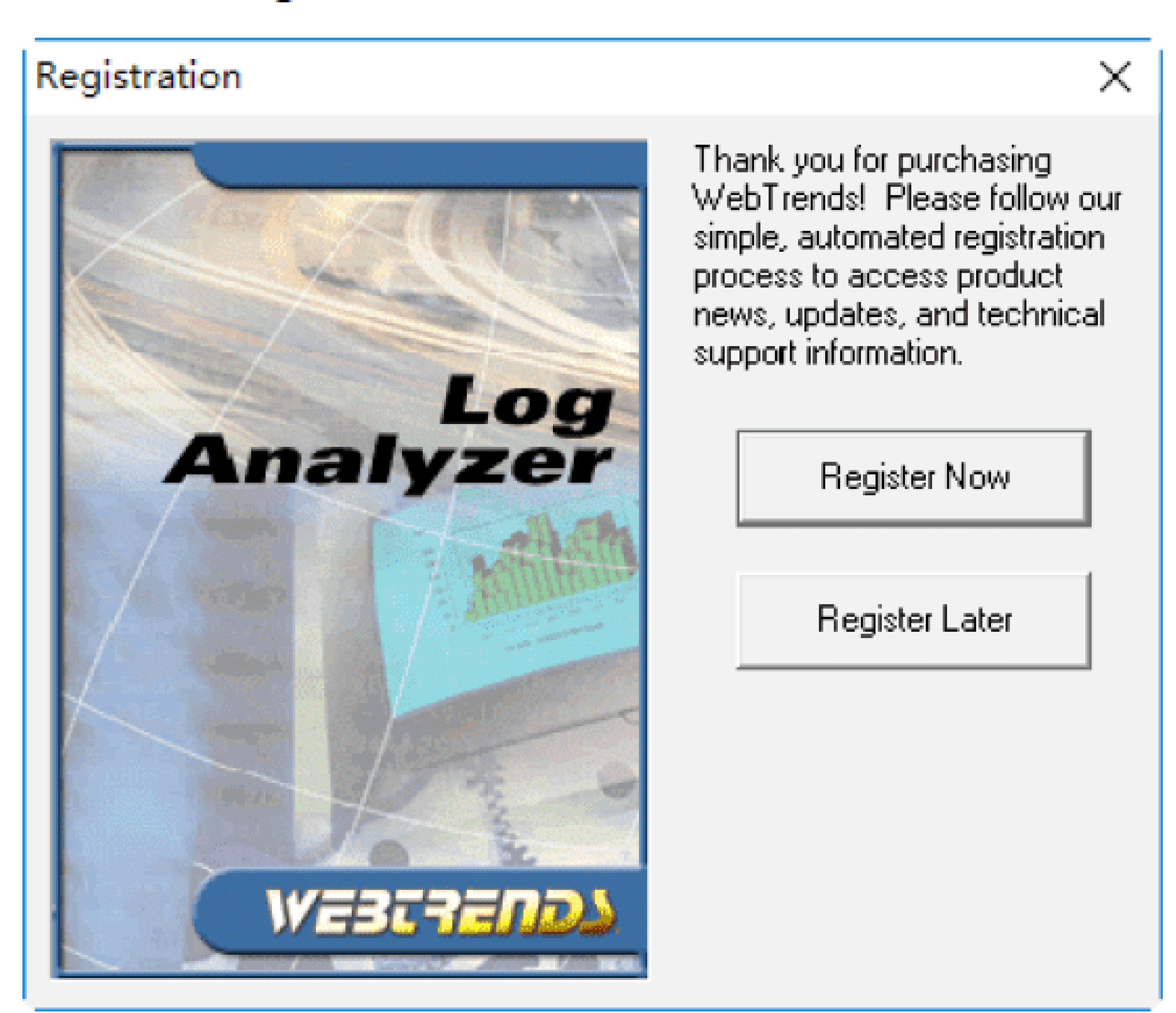
Step 02 单击Submit按钮，如果看到“添加序列号成功”提示，则说明该序列号是可用的，如下图所示。



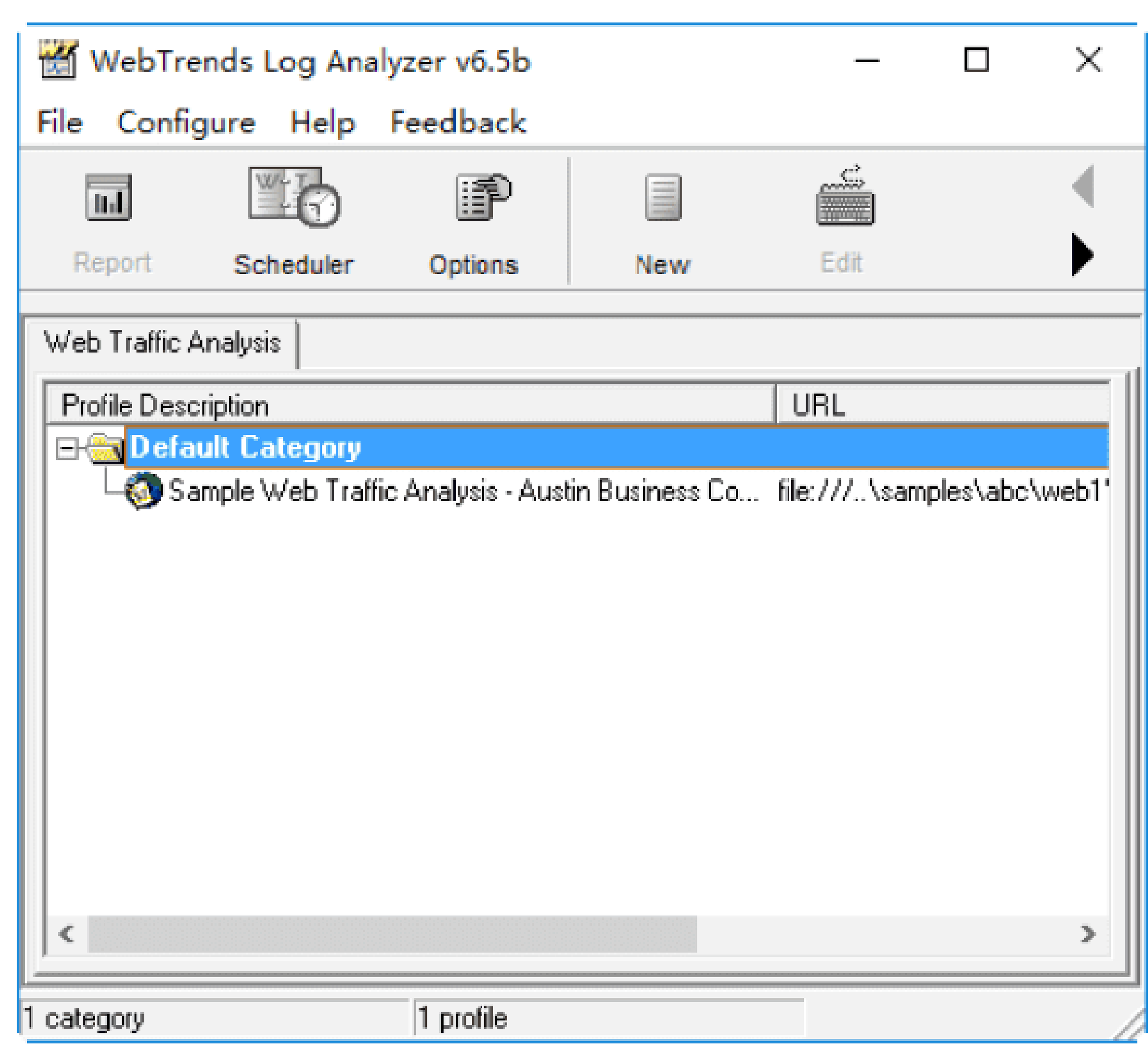
Step 03 单击“确定”按钮之后，单击Exit按钮，即可看到Proferer WebTrends窗口，如下图所示。



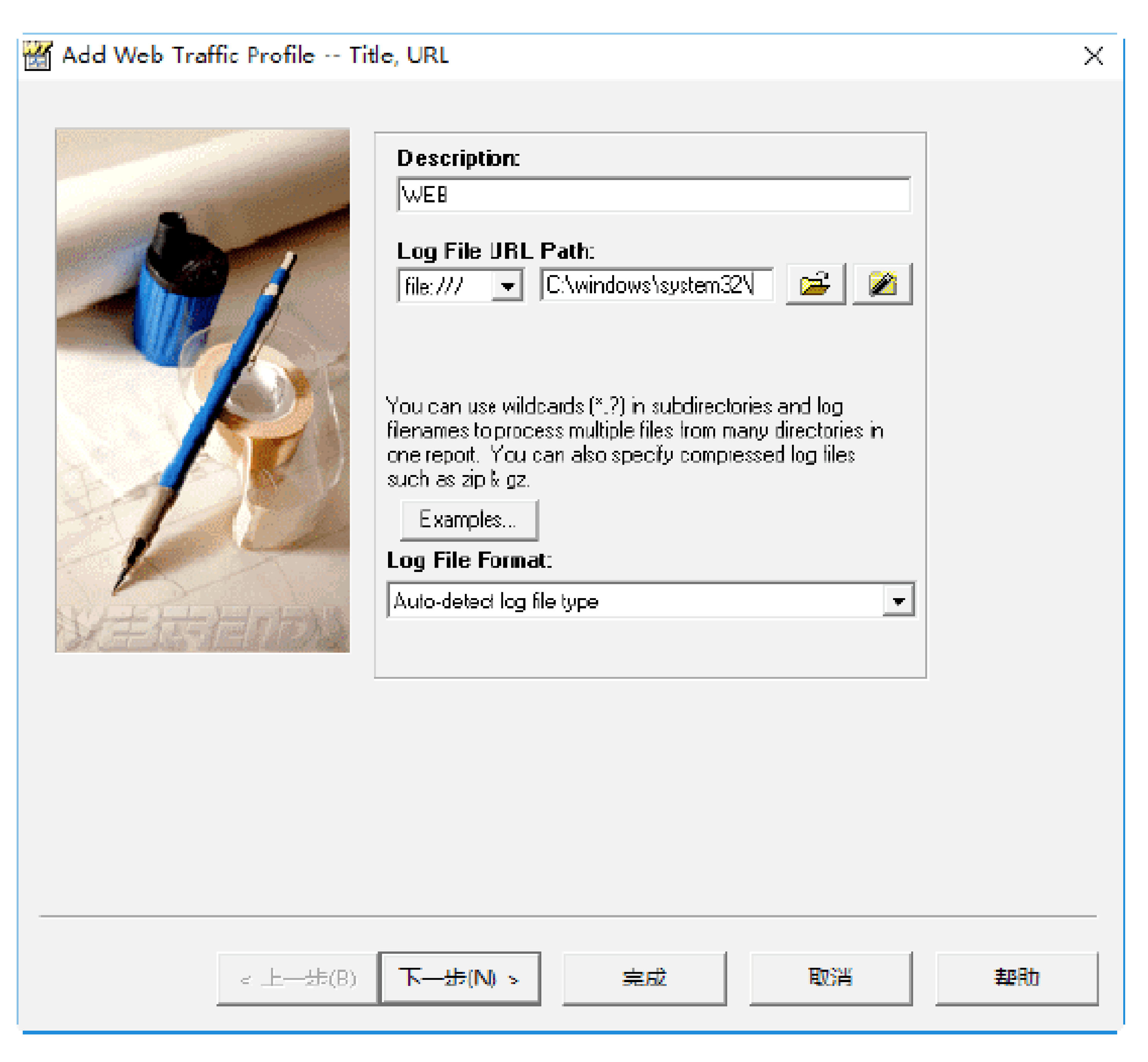
Step 04 单击Start Using the Product按钮，即可打开Registration对话框，如下图所示。



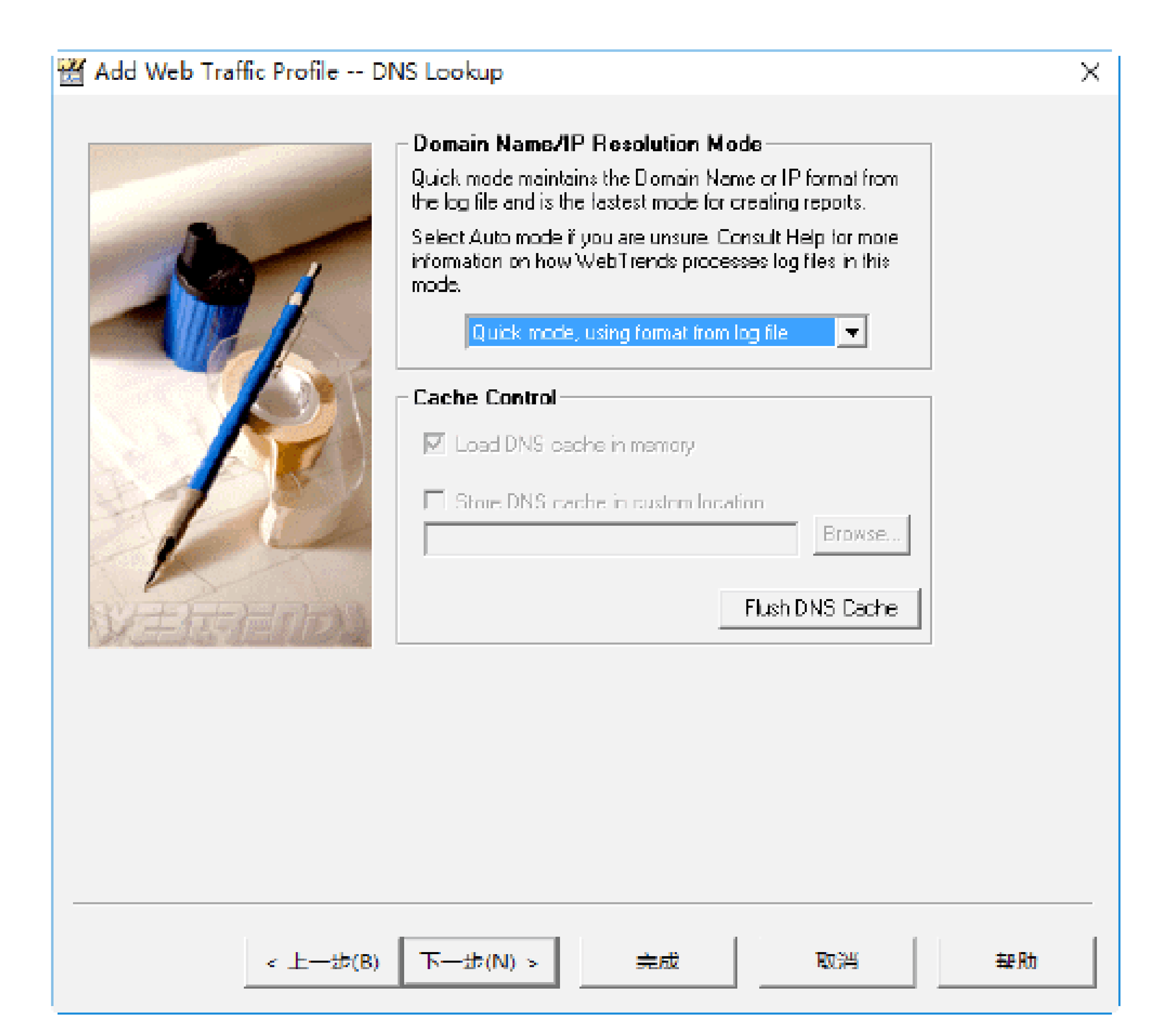
Step 05 单击Register Later按钮，打开WebTrends Log Analyzer v6.5b主窗口，如下图所示。



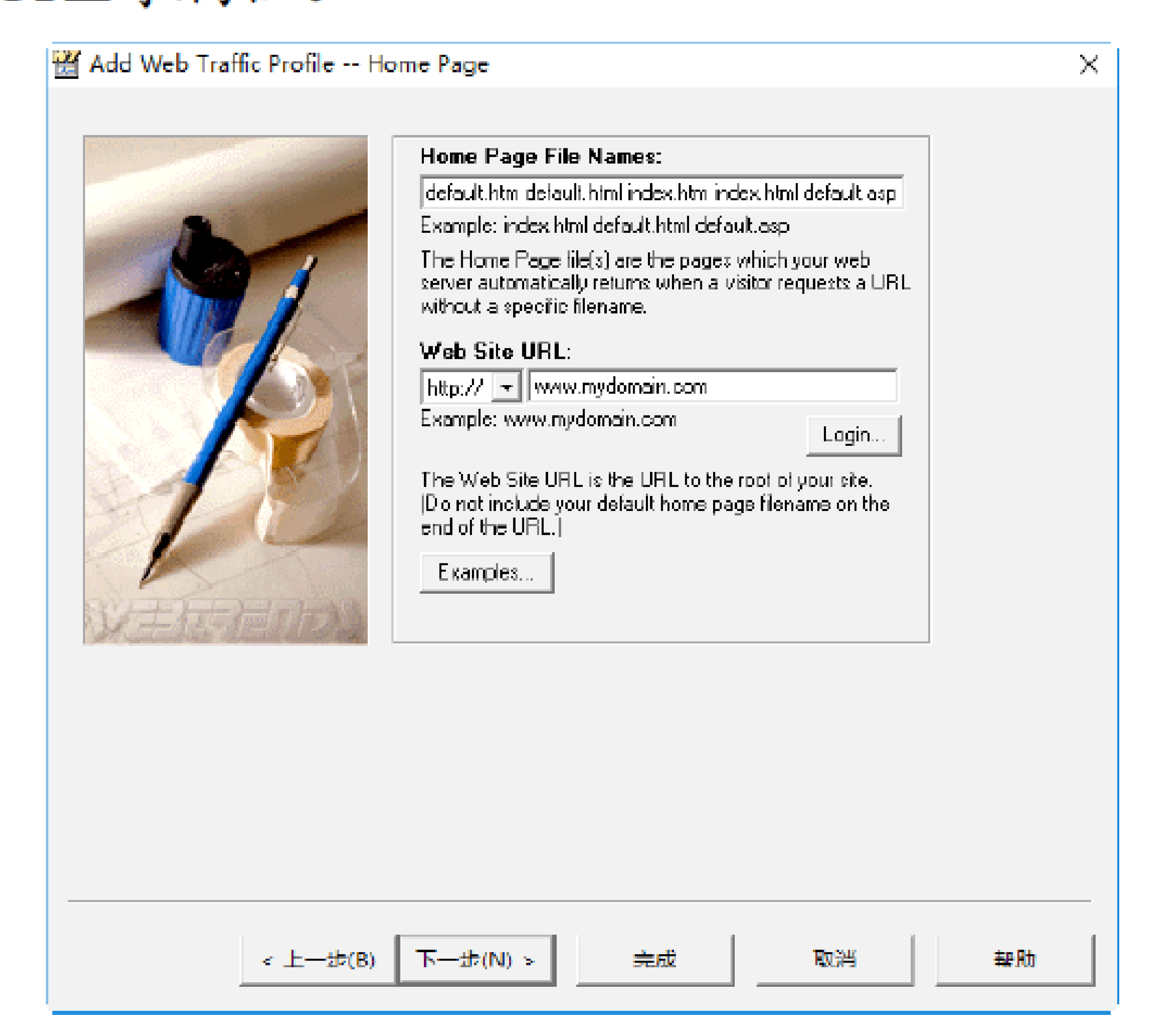
Step 06 单击New按钮，打开如下图所示的对话框，在Description文本框中输入准备访问日志的服务器类型名称；在Log File URL Path下拉列表中选择存放方式，在后面的文本框中输入相应的路径；在Log File Format下拉列表中可以看到WebTrends支持多种日志格式，这里选择Auto-detect log file type选项。



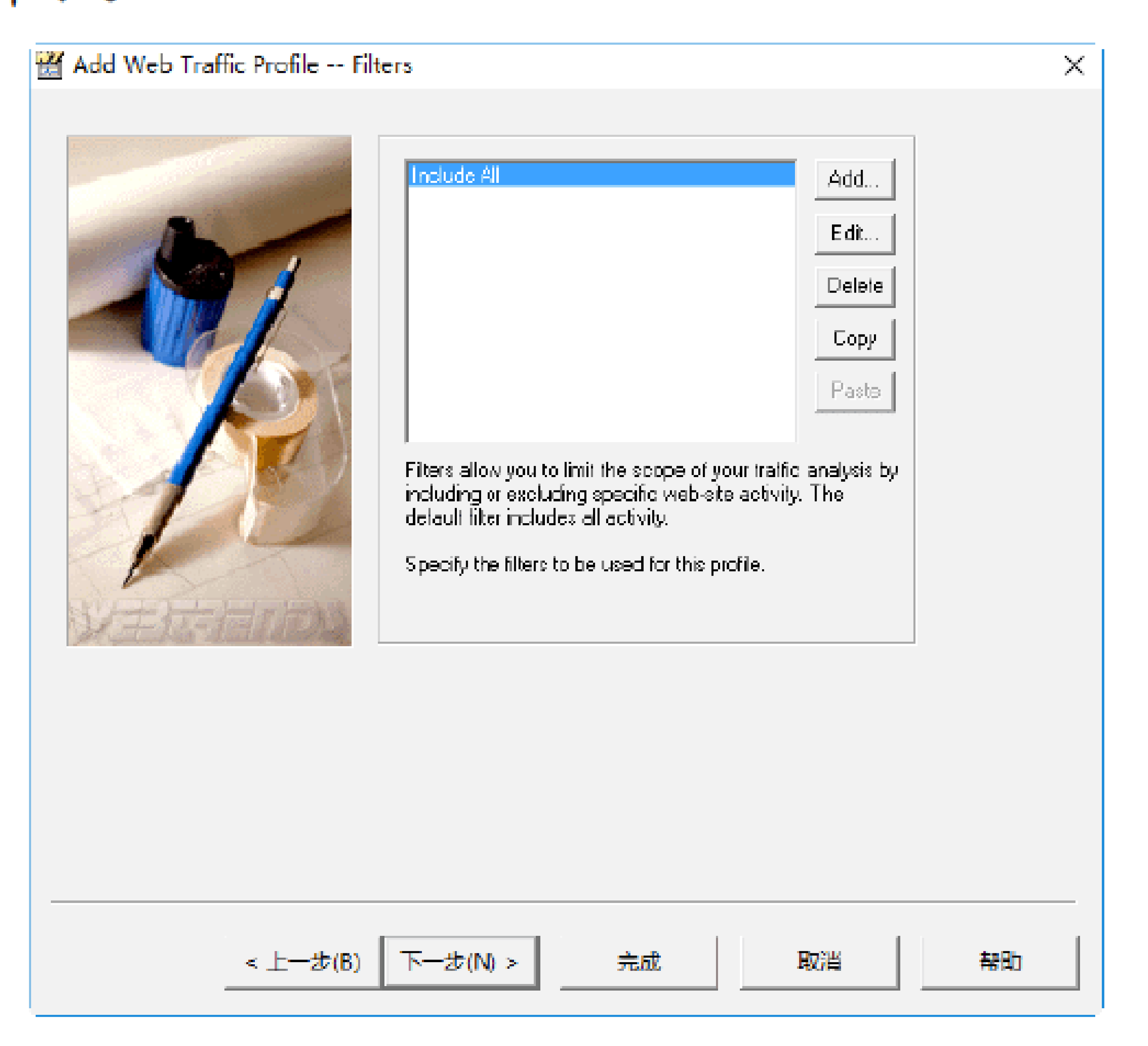
Step 07 单击“下一步”按钮，打开如下图所示的对话框，在其中可以设置站点的日志IP采用查询DNS的方式，如下图所示。



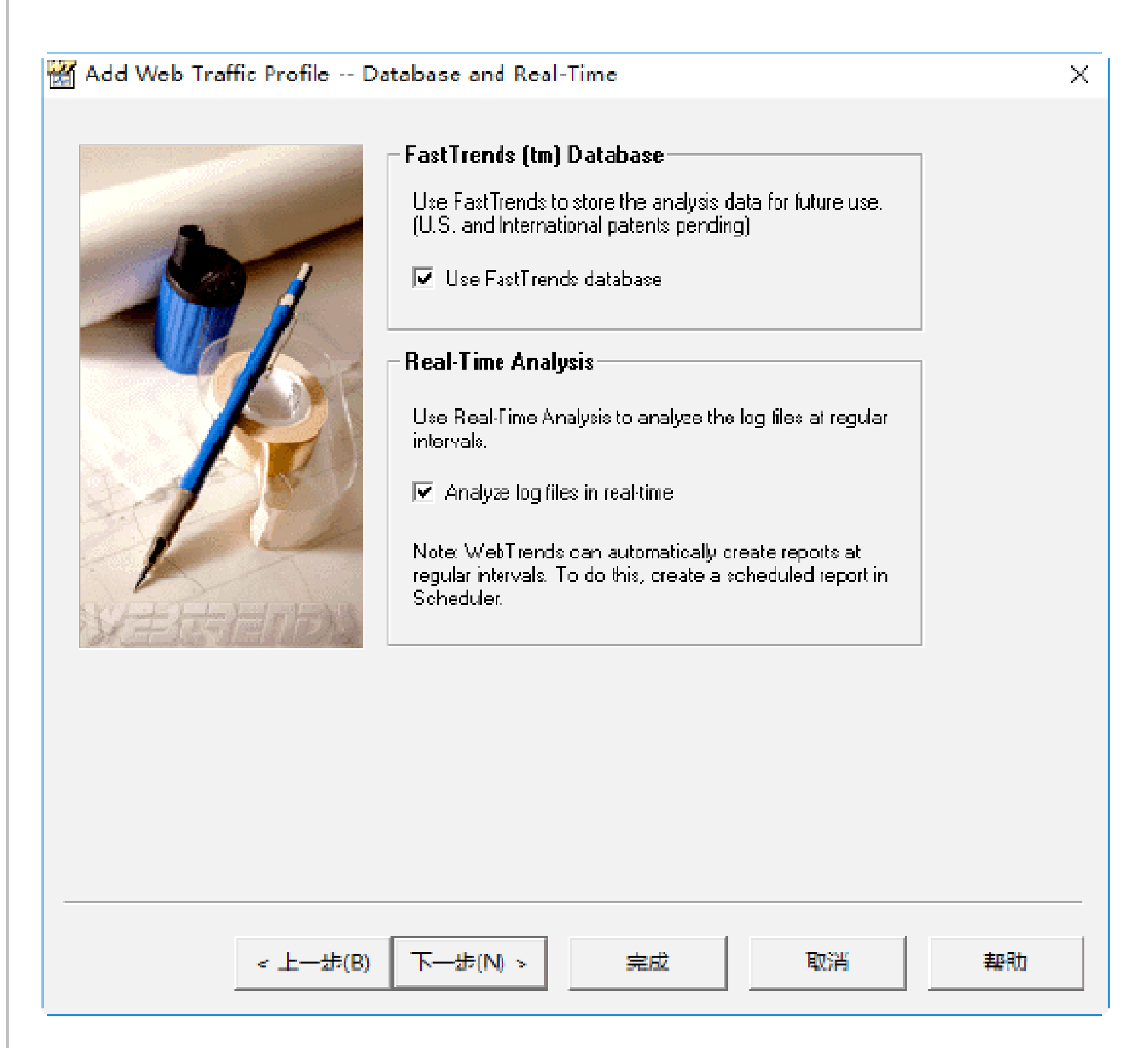
Step 08 单击“下一步”按钮，打开如下图所示的对话框，在其中设置站点的首页文件和URL等属性。



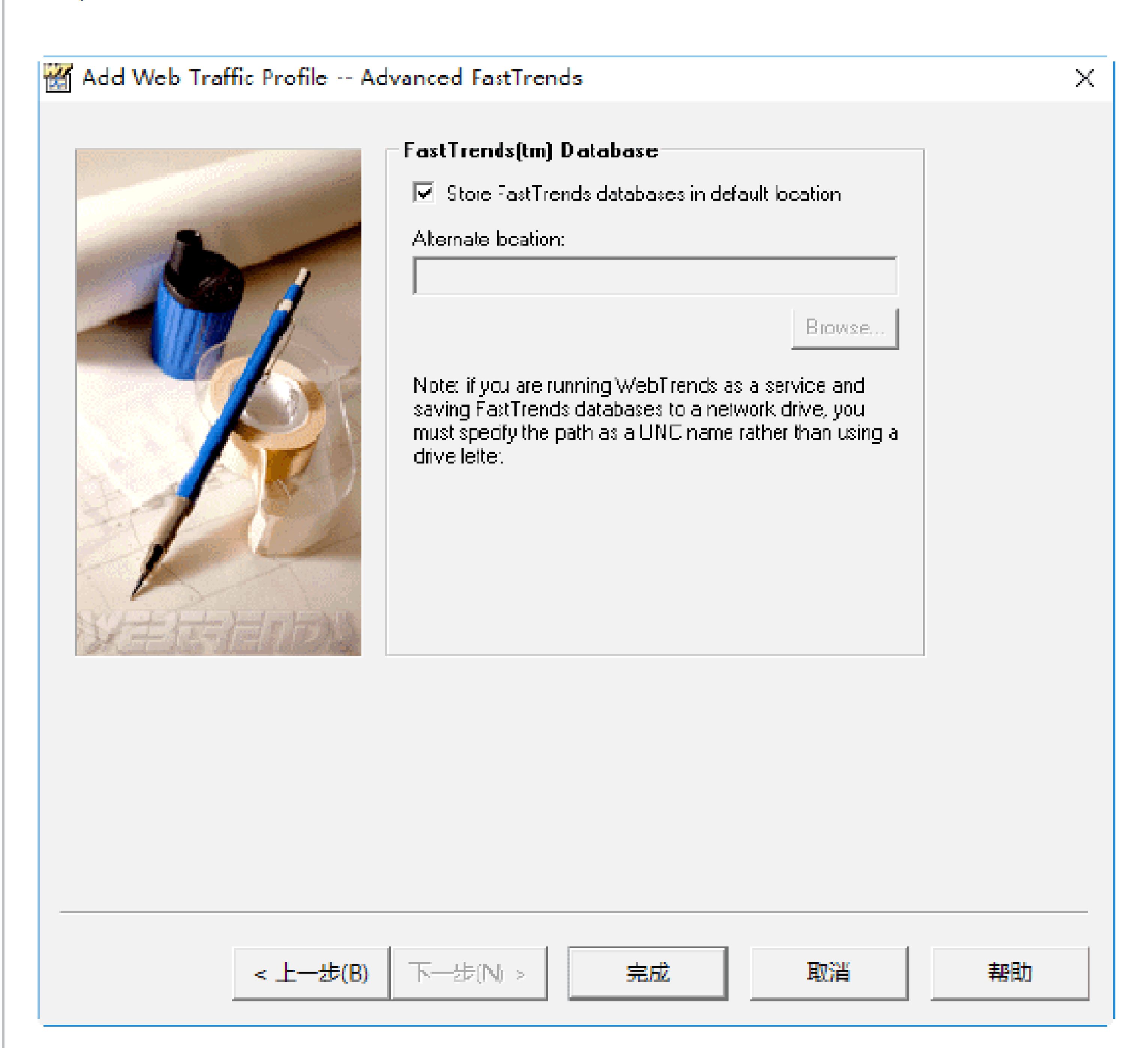
Step 09 单击“下一步”按钮，打开如下图所示的对话框，在其中需要设置WebTrend对站点中哪些类型的文件做日志，这里默认的是所有文件类型（Include all），如下图所示。



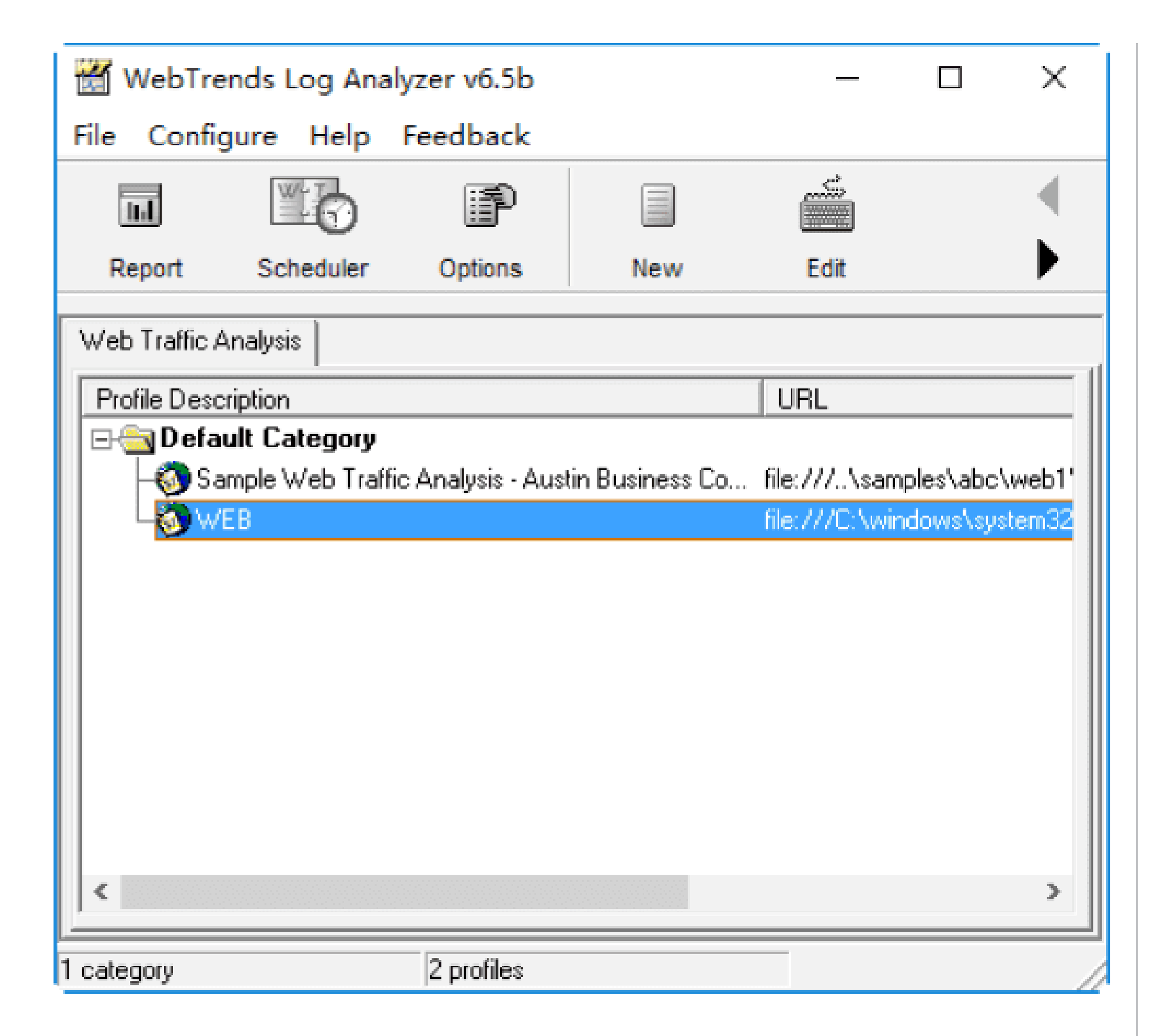
Step 10 单击“下一步”按钮，打开如下图所示的对话框，在其中勾选Use FastTrends database复选框和Analyze log file in real-time复选框，如下图所示。



Step 11 单击“下一步”按钮，打开如下图所示的对话框，这里勾选Store Fast Trends databases in default location复选框，如下图所示。



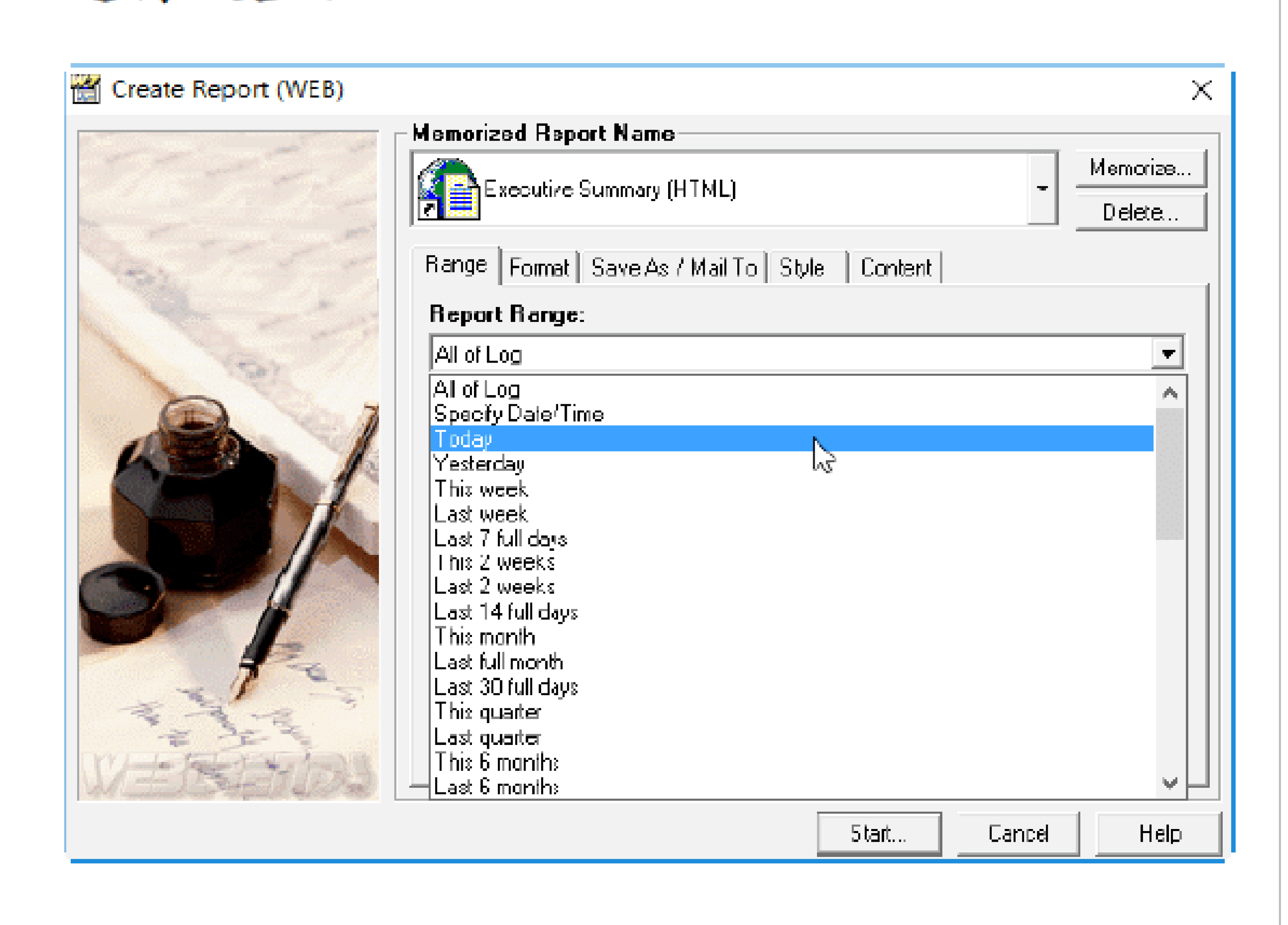
Step 12 单击“完成”按钮，即可完成新建日志站点，在WebTrends Log Analyzer v6.5b窗口可看到新创建的Web站点，如下图所示。



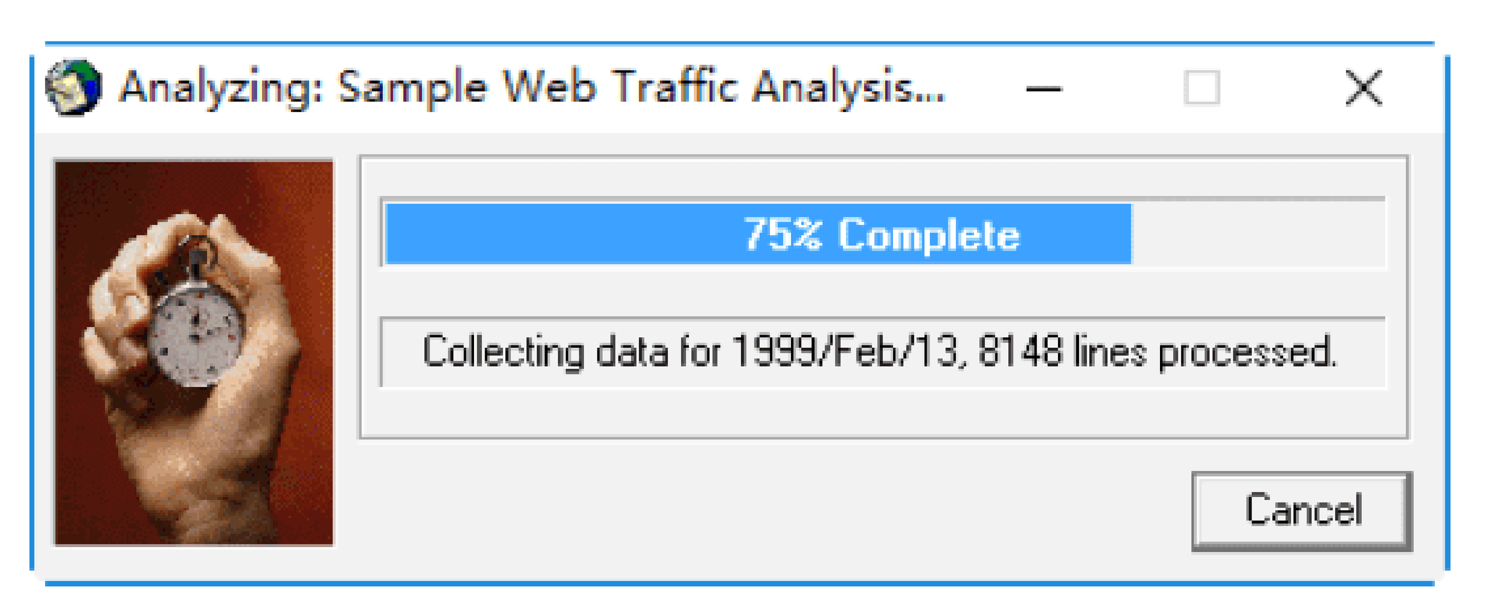
实战3：使用WebTrends生成日志报表

一个日志站点创建完成后，等待一定访问量后就可以对指定的目标主机进行日志分析并生成日志报表了，具体的操作步骤如下。

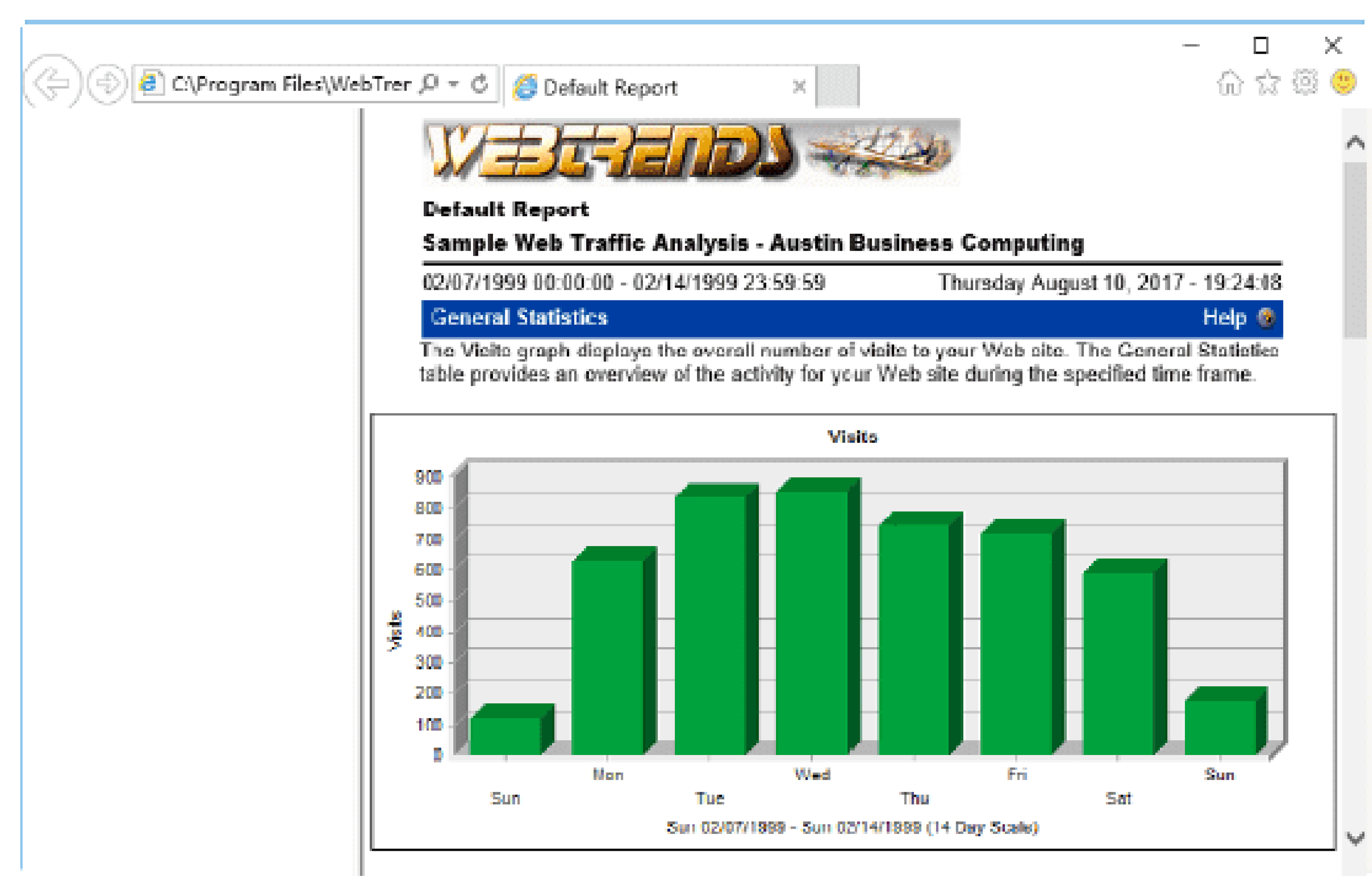
Step 01 在WebTrends Log Analyzer主窗口单击工具栏中的Report按钮，打开Create Report（WEB）对话框，在Report Range列表中可以看到WebTrends提供多种日志的产生时间以供选择，这里选择所有的日志，如下图所示。另外，还需要对报告的风格、标题、文字、显示哪些信息（如访问者IP、访问时间、访问内容等）等信息进行设置。



Step 02 单击Start按钮，即可对选择的日志站点进行分析并生成报告，如下图所示。



Step 03 待分析完毕后，即可看到以HTML形式的报告，在其中可以看到该站点的各种日志信息，如下图所示。



15.3　清除服务器入侵日志

黑客在入侵服务器的过程中，其操作会留下痕迹，那么清除日志是黑客入侵后必须要做的一件事情，本节主要讲述如何清除这些痕迹。下面详细介绍黑客是通过什么样的方法把记录自己痕迹的日志删除掉的。

实战4：清除WWW日志和FTP日志信息

黑客在对目标服务器实施入侵之后，为了防止网络管理员对其进行追踪，往往要删除留下的IP记录和FTP记录，但这种系统日志用手工的方法很难清除，这时需要借助于其他软件进行清除。在Windows系统中，WWW日志一般都存放在%winsys-tem%\sys tem32\logfiles\w3svc1文件夹中，包括WWW日志和FTP日志。

Windows 10系统中一些日志存放路径和文件名如下。

（1）安全日志：C:\windows\system\sys-tem32\config\Secevent.evt。

（2）应用程序日志：C:\windows\system\system32\config\AppEvent.evt。

（3）系统日志：C:\windows\winsystem\system32\config\SysEvent.evt。

（4）IIS的FTP日志：C:\windows\system%\system32\logfiles\msftpsvc1\，默认每天一个日志。

（5）IIS的WWW日志：C:\windows\system\system32\logfiles\w3svc1\，默认每天一个日志。

（6）Scheduler服务日志：C:\windows\winsystem\schedlgu.txt。

（7）注册表项目：[HKLM]\system\CurrentControlSet\Services\Eventlog。

（8）Schedluler服务注册表所在项目：[HKLM]\SOFTWARE\Microsoft\SchedulingAgent。

1. 清除WWW日志

在IIS中WWW日志默认的存储位置是C:\windows\system\system32\logfiles\w3svc1\，每天都产生一个新日志。如果管理员对其存放位置进行了修改，则可以运用iis.msc对其进行查看，再通过查看网站的属性来查找到其存放位置，此时，就可以在“命令提示符”窗口通过del *.*命令清除日志文件。

但这个方法删除不掉当天的日志，这是因为w3svc服务还在运行着。可以用net stop w3vsc命令把这个服务停止之后，再用del *.*命令，就可以清除当天的日志了。

另外，还可以用记事本把日志文件打开，删除其内容之后再进行保存，也可以清除日志。最后用net start w3svc命令再启动w3svc服务就可以了。

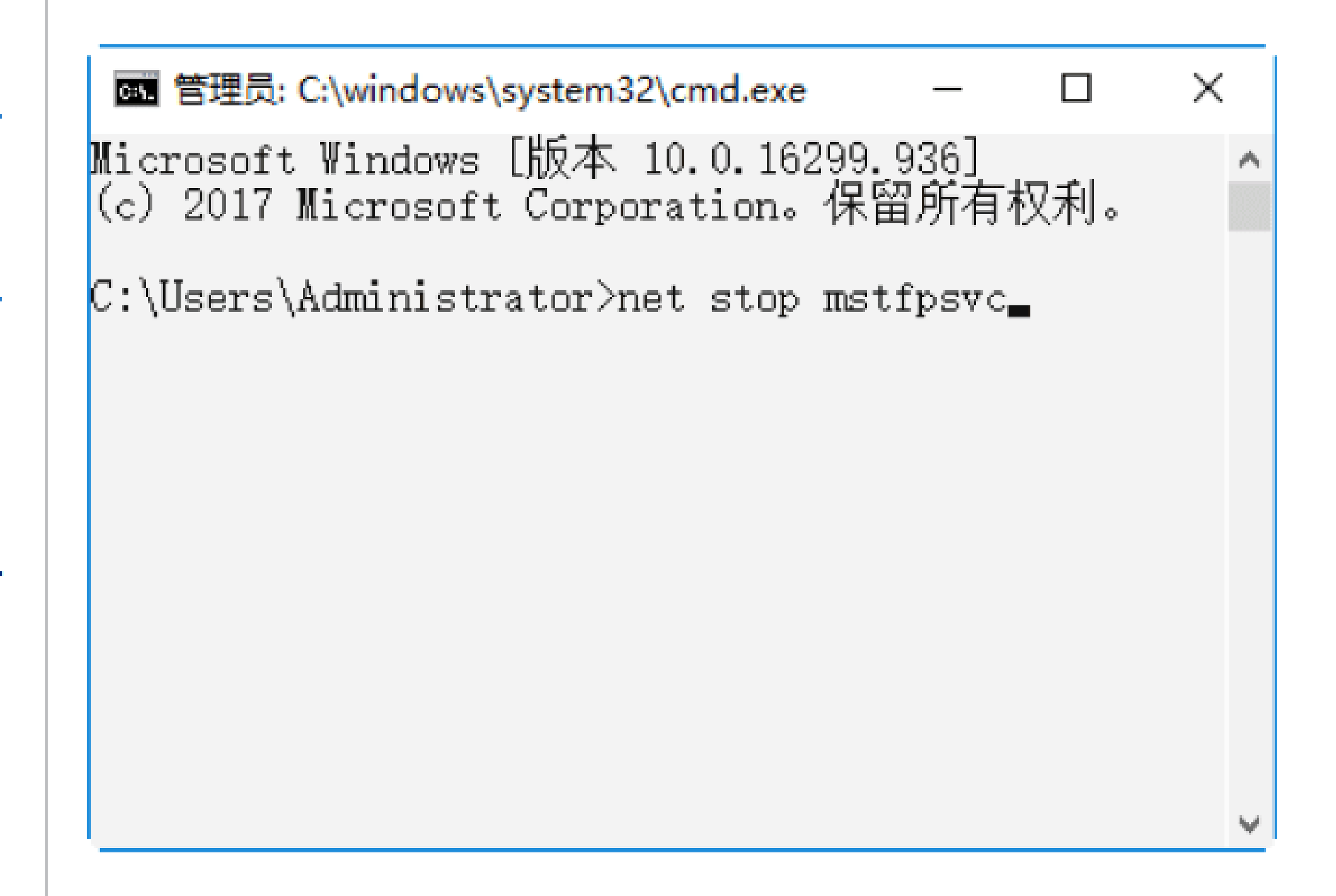
提示：删除日志前必须先停止相应的服务，再进行删除即可。日志删除后务必要记得再打开相应的服务。

2. 清除FTP日志

FTP日志的默认存储位置为C:\windows\system\system32\logfiles\msftpsvcl\，其清除方法和清除WWW日志的方法差不多，只是所要停止的服务不同。

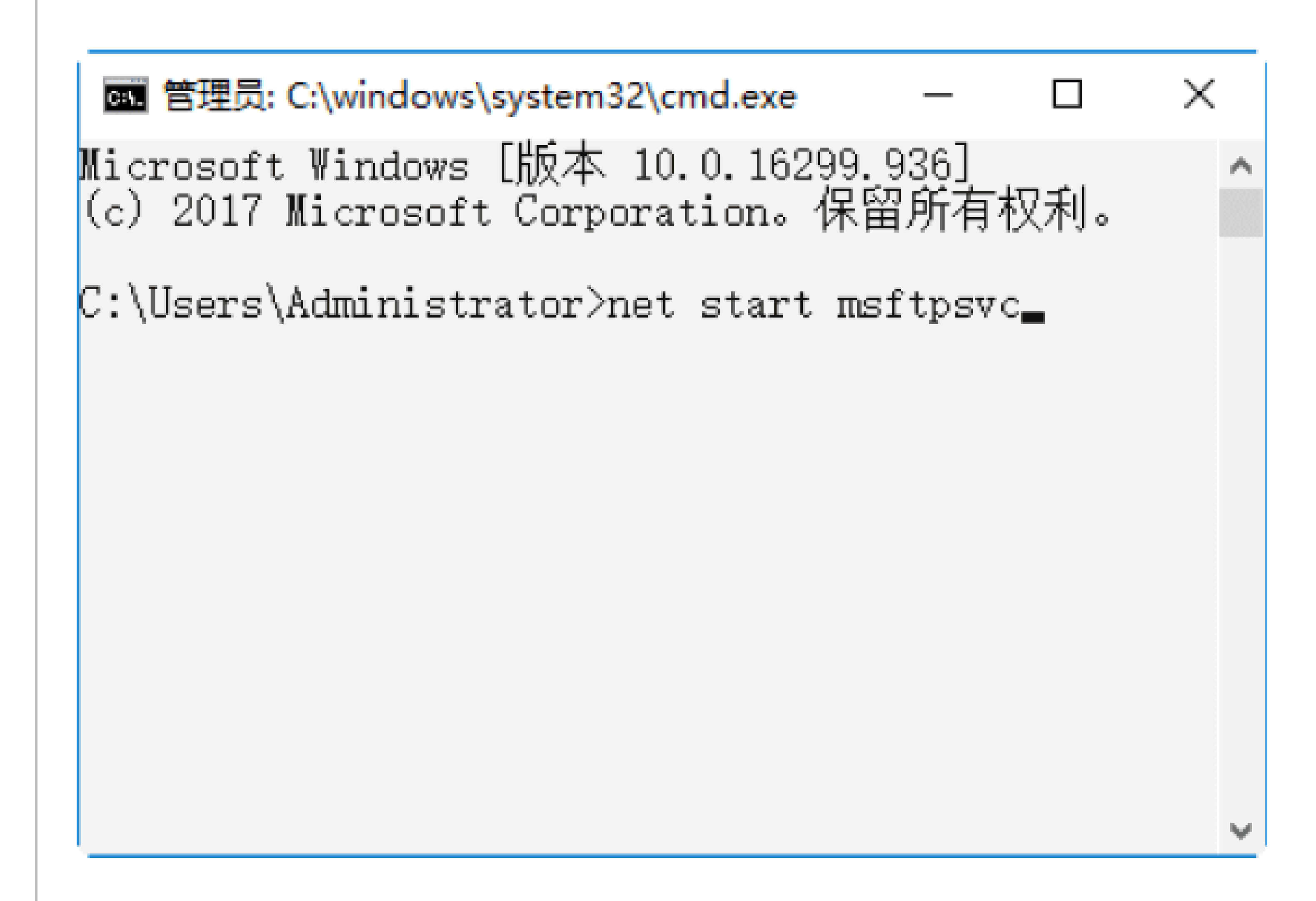
清除FTP日志的具体操作步骤如下。

Step 01 在“命令提示符”窗口中运行net stop mstfpsvc命令，即可停掉msftpsvc服务，如下图所示。



Step 02 运行del *.*命令或找到日志文件，并将其内容删除。

Step 03 运行net start msftpsvc命令，再打开msftpsvc服务即可，如下图所示。



提示：也可修改目标计算机中的日志文件，其中WWW日志文件存放在w3svc1文件夹下，FTP日志文件存放在msftpsvc1文件夹下，每个日志都是以ex.log为命名的（其中X代表日期）。

实战5：使用批处理清除日志信息

在一般情况下，日志会忠实地记录它接收到的任何请求，用户会通过查看日志来发现入侵的企图，从而保护自己的系统。所以黑客在入侵系统成功后，首先便是清除该计算机中的日志，擦去自己的形迹。除手工删除外，还可以通过创建批处理文件来删除日志。

具体的操作步骤如下。

Step 01 在记事本中编写一个可以清除日志的批处理文件，其具体内容如下。

```
@del C:\Windows\system32\logfiles\*.*
@del C:\Windows \system32\config\*.
evt
@del C:\Windows \system32\dtclog\*.*
@del C:\Windows \system32\*.log
@del C:\Windows \system32\*.txt
@del C:\Windows \*.txt
@del C:\Windows t\*.log
@del c:\del.bat
```

Step 02 把上述内容保存为del.bat备用，再新建一个批处理文件并将其保存为clear.bat文件，其具体内容如下。

```
@copy del.bat \\1\c$
@echo 向主机复制本机的del.bat……OK
@psexec \\1 c:\del.bat
@echo 在主机上运行del.bat，清除日志文
件……OK
```

上述代码中echo是DOS下的回显命令，在它的前面加上“@”前缀字符，表示执行时本行在命令行或DOS里面不显示，它是删除文件命令。

Step 03 假设已经与主机进行了IPC连接，在“命令提示符”窗口中输入clear.bat 192.168.0.10命令，即可清除该主机上的日志文件。

15.4 实战演练

实战演练1——使用事件查看器分析日志信息



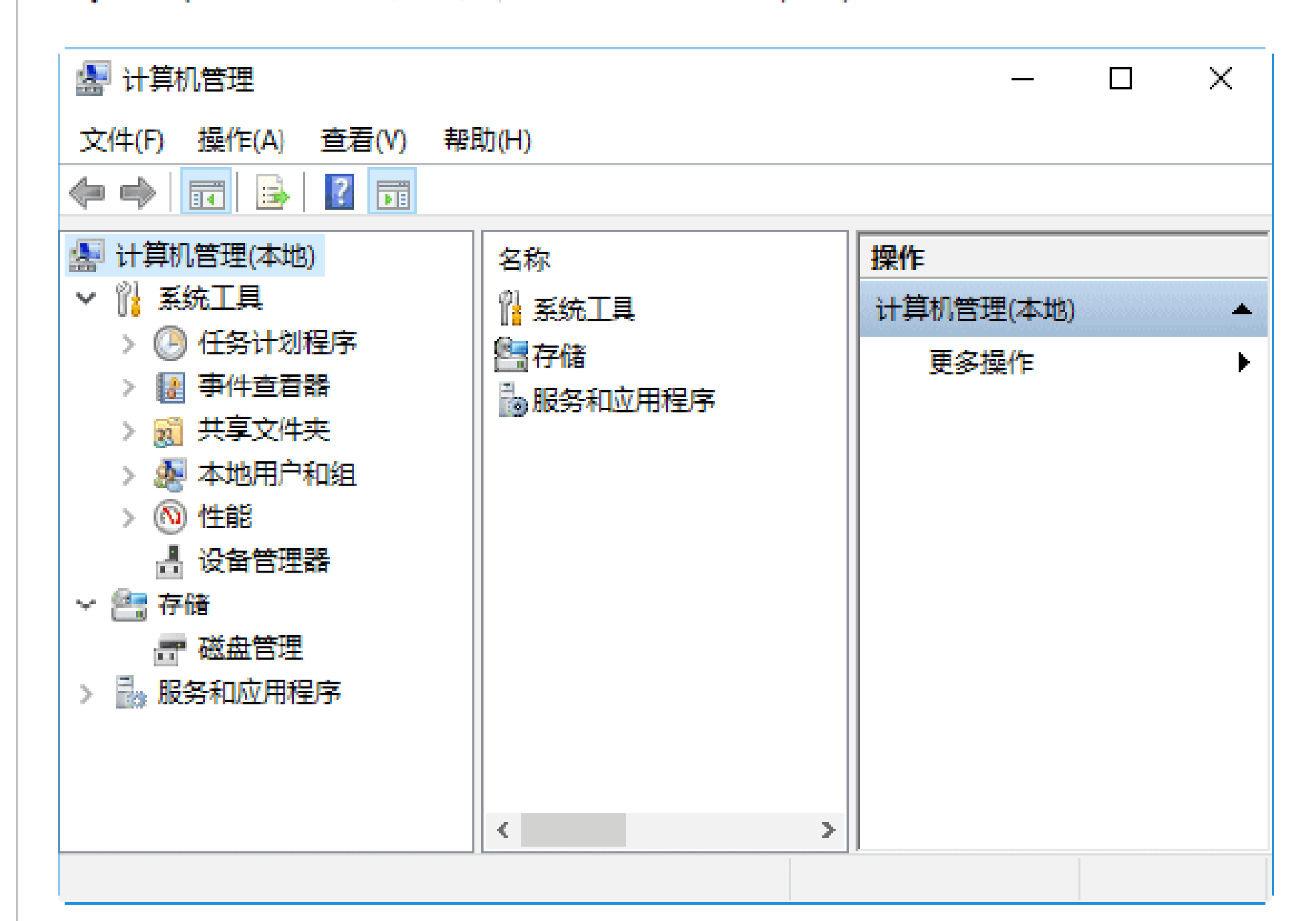
不管是不是计算机高手，都要学会根据Windows自带的“事件查看器”对应用程序、系统、安全和设置等进程进行分析与管理。

通过事件查看器查找间谍软件的操作步骤如下。

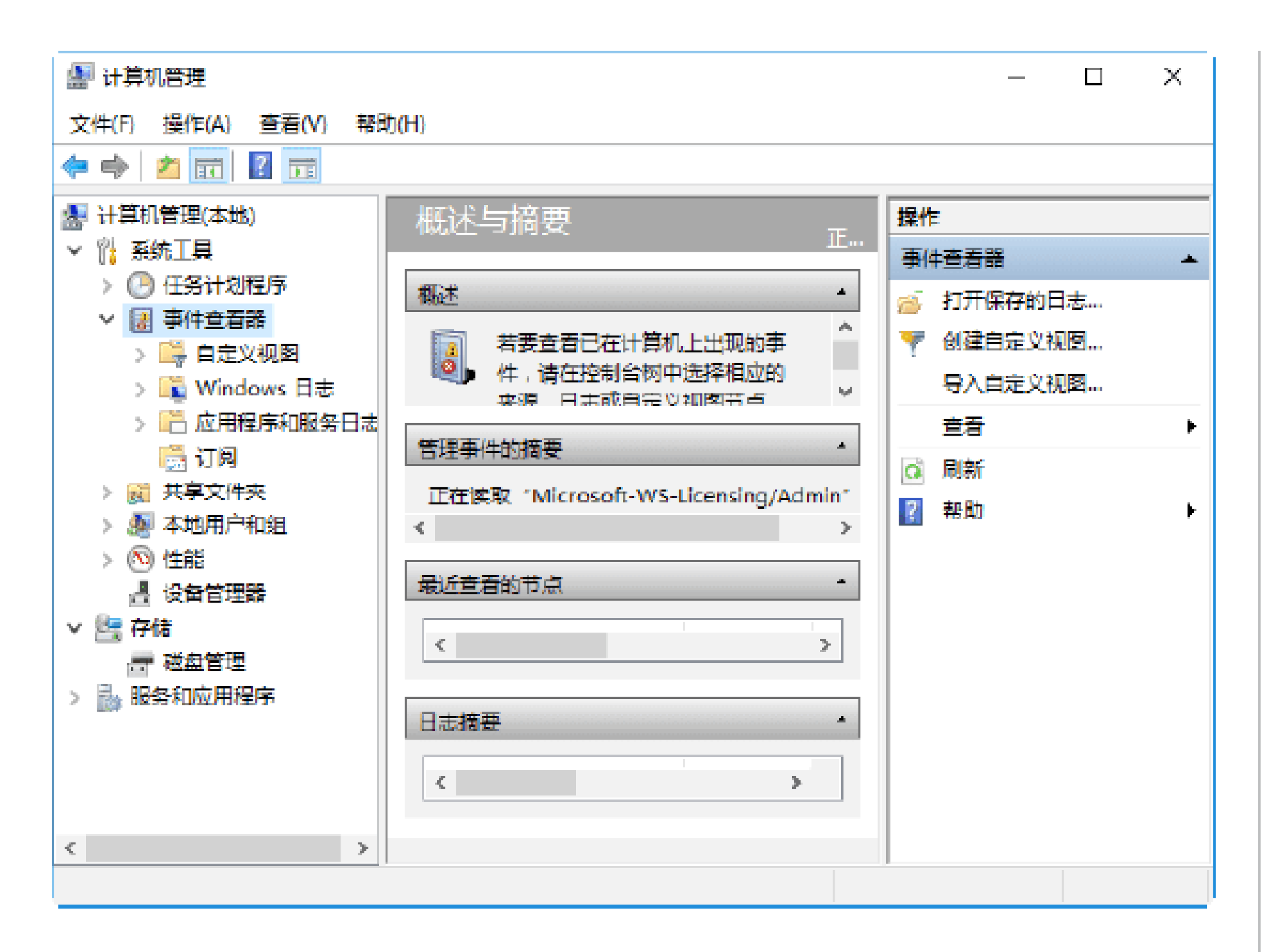
Step 01 右击“此计算机”图标，在弹出的快捷菜单中选择“管理”选项，如下图所示。



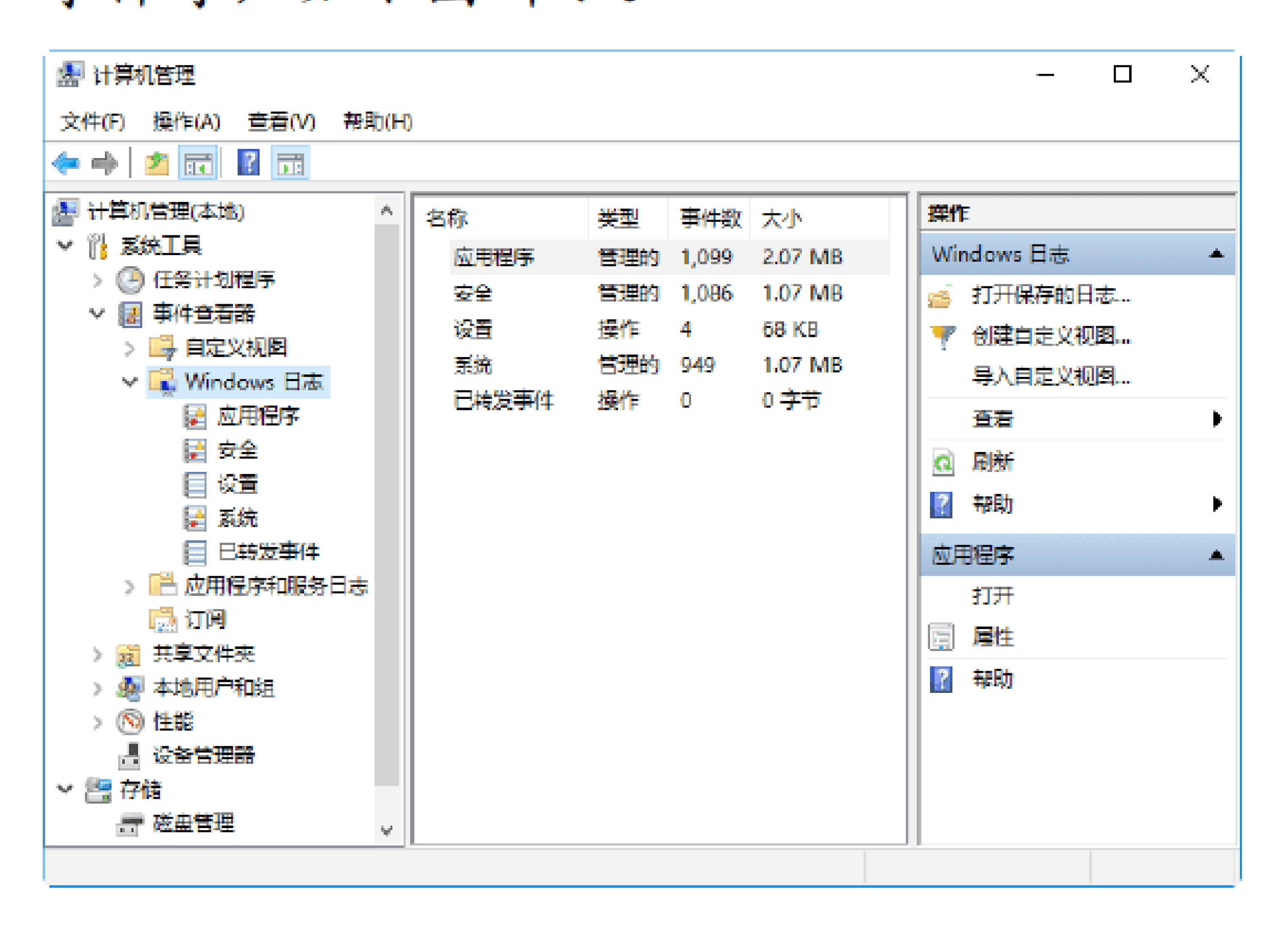
Step 02 弹出“计算机管理”对话框，在其中可以看到系统工具、存储、服务和应用程序3个方面的内容，如下图所示。



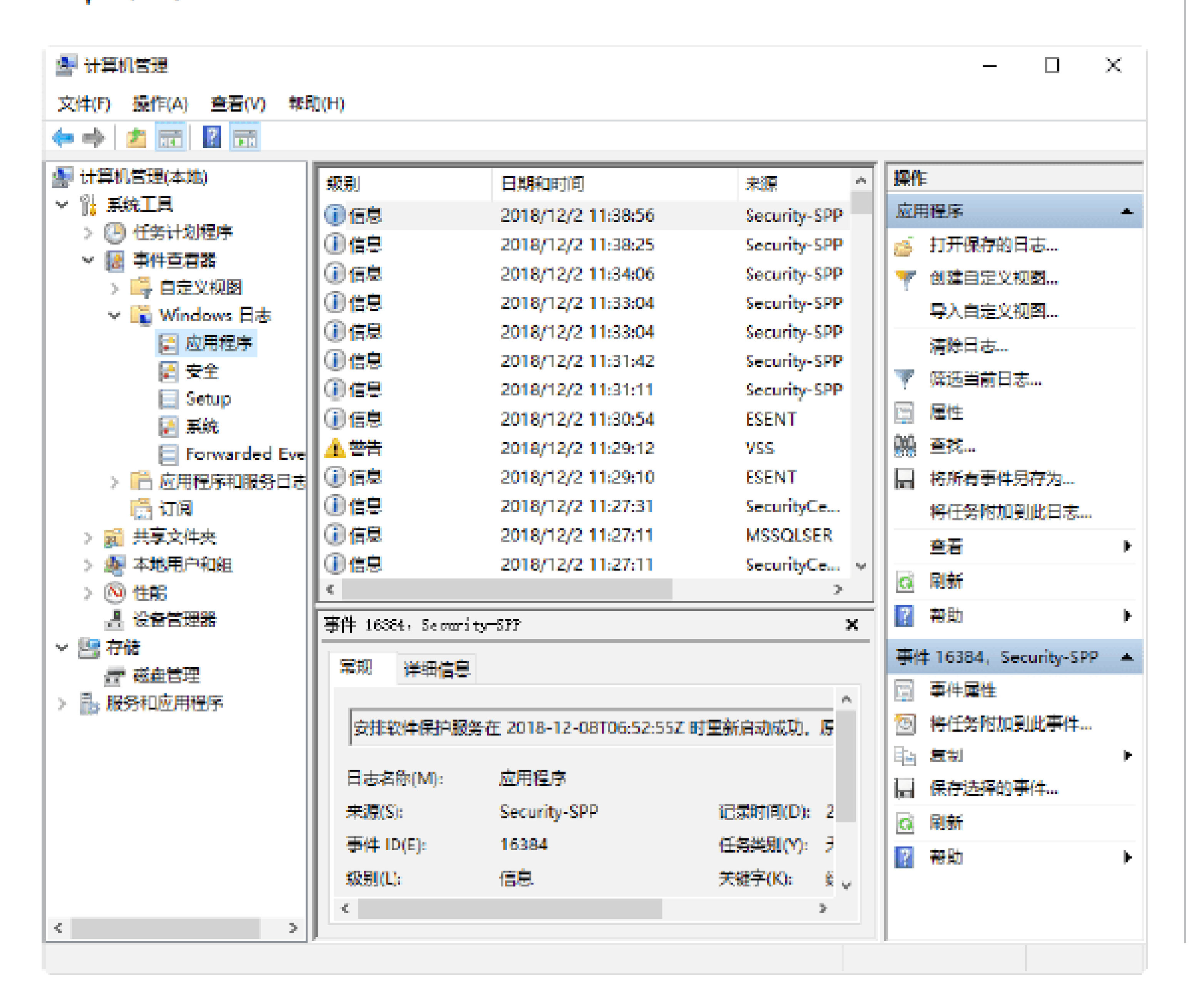
Step 03 在左侧依次展开“计算机管理（本地）”→“系统工具”→“事件查看器”选项，即可在下方显示事件查看器所包含的内容，如下图所示。



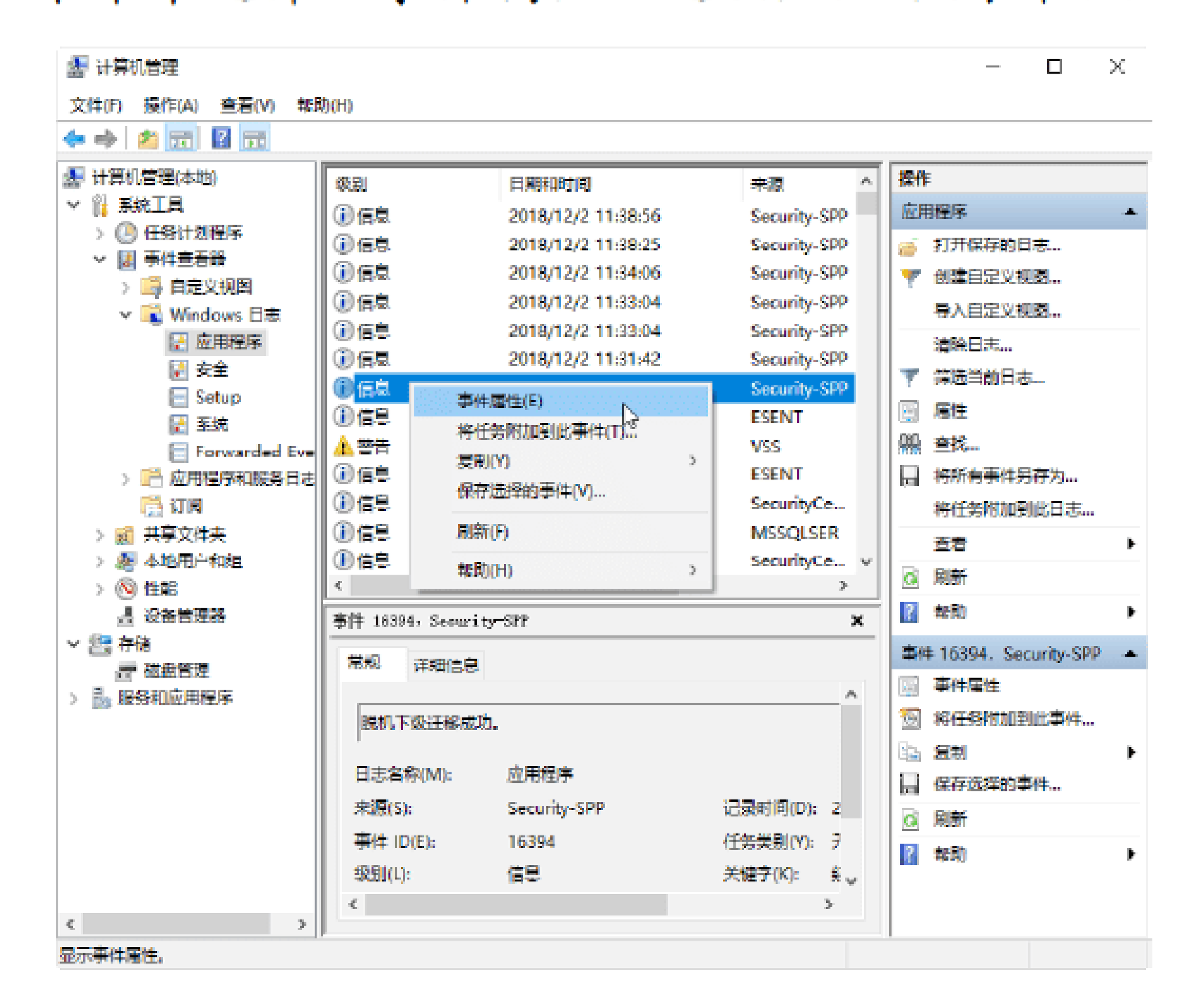
Step 04 双击“Windows日志”选项，即可在右侧显示有关Windows日志的相关内容，包括应用程序、安全、设置、系统和已转发事件等，如下图所示。



Step 05 双击右侧区域中的“应用程序”选项，即可在打开的界面中看到非常详细的应用程序信息，其中包括应用程序被打开、修改、权限过户、权限登记、关闭以及重要的出错或者兼容性信息等，如下图所示。



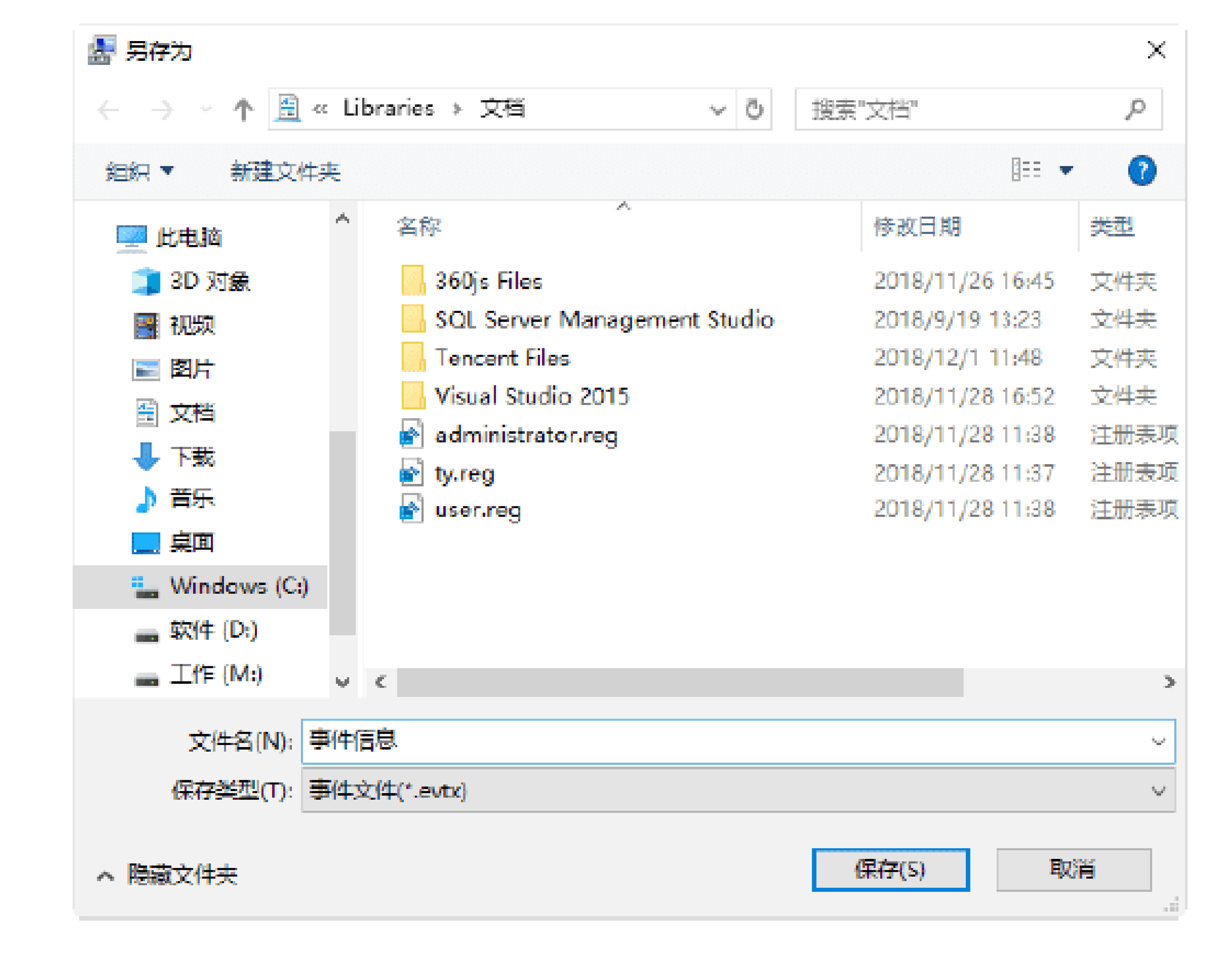
Step 06 右击其中任意一条信息，在弹出的快捷菜单中选择“事件属性”选项，如下图所示。



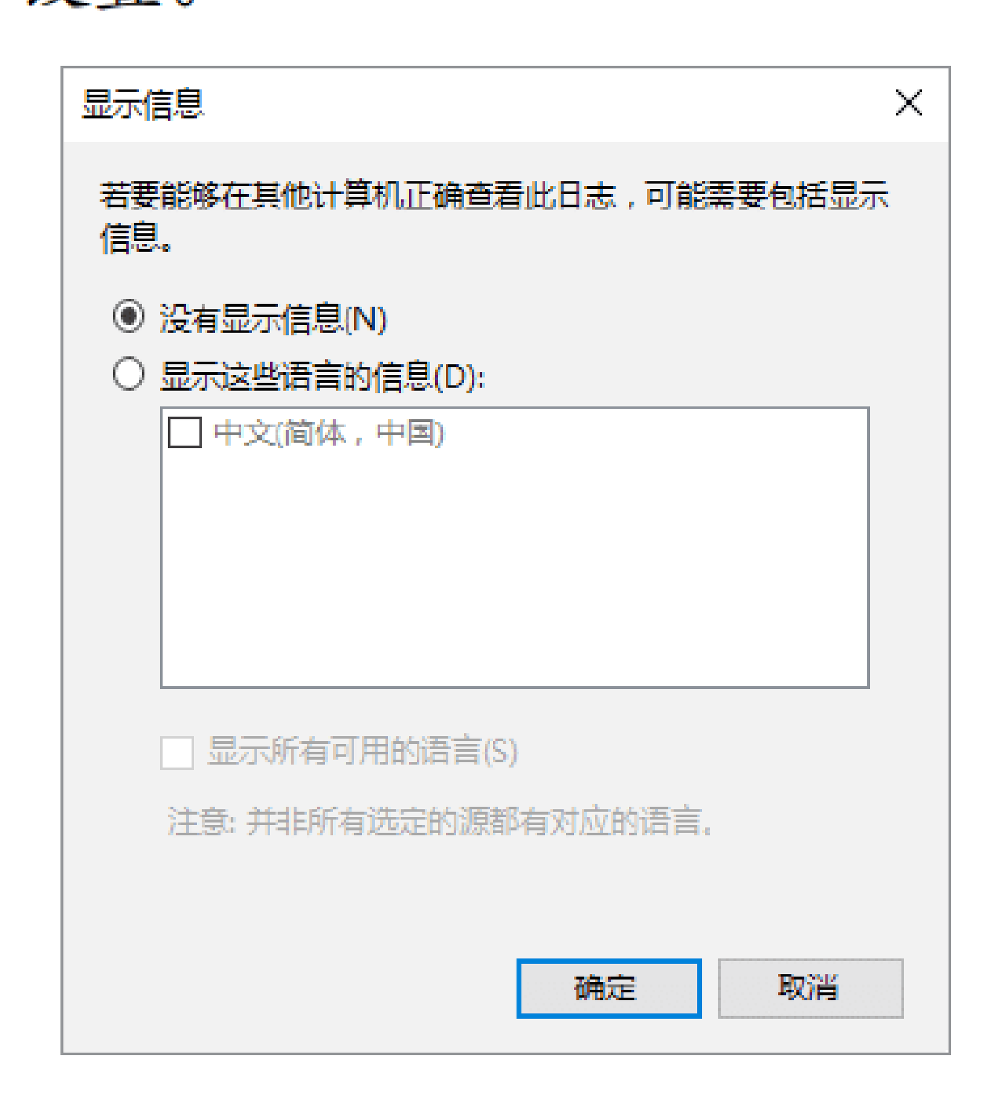
Step 07 打开“事件属性”对话框，在该对话框中可以查看该事件的常规属性以及详细信息等，如下图所示。



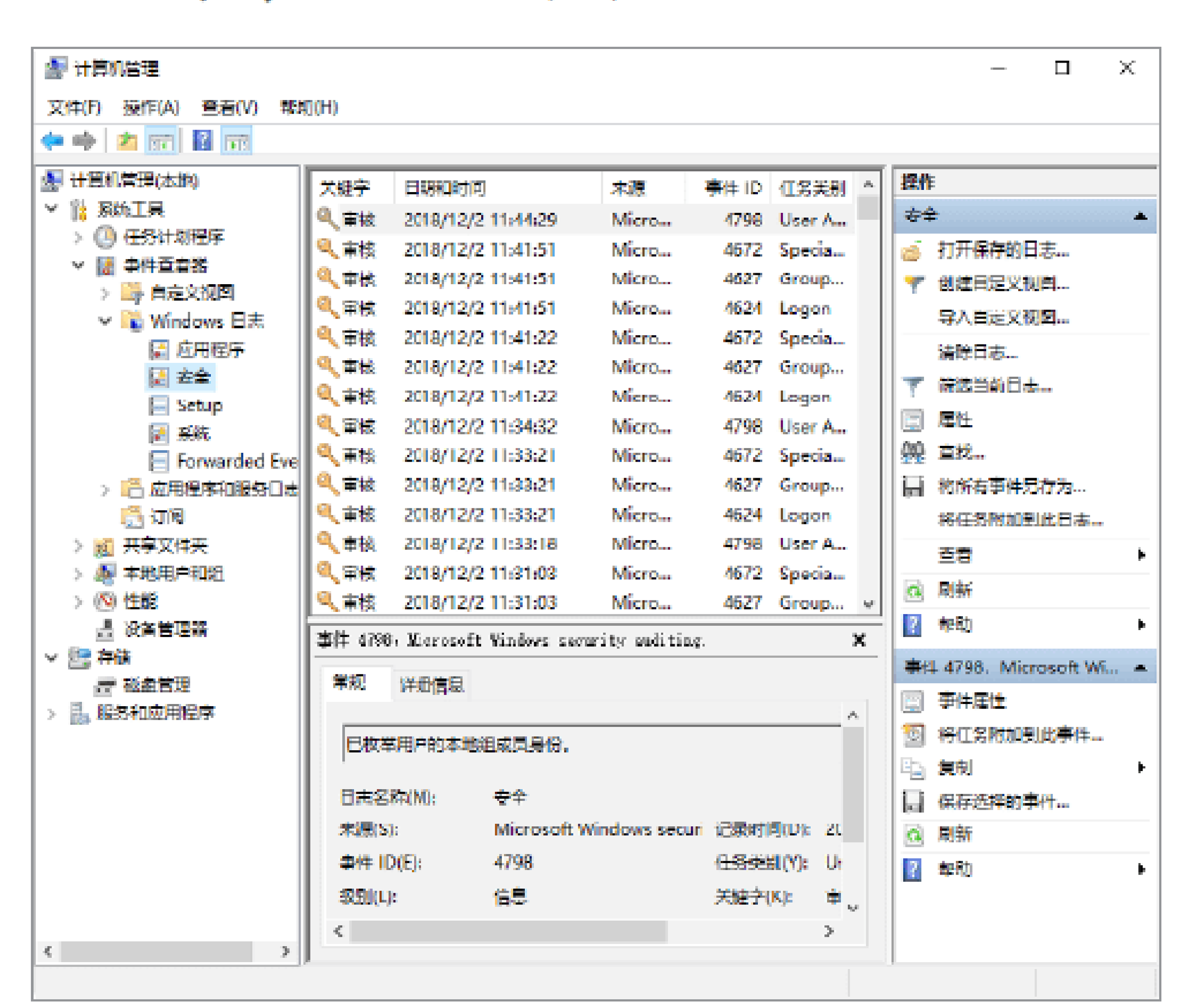
Step 08 右击其中任意一条应用程序信息，在弹出的快捷菜单中选择“保存选择的事件”选项，弹出“另存为”对话框，在“文件名”文本框中输入事件的名称，并选择事件保存的类型，如下图所示。



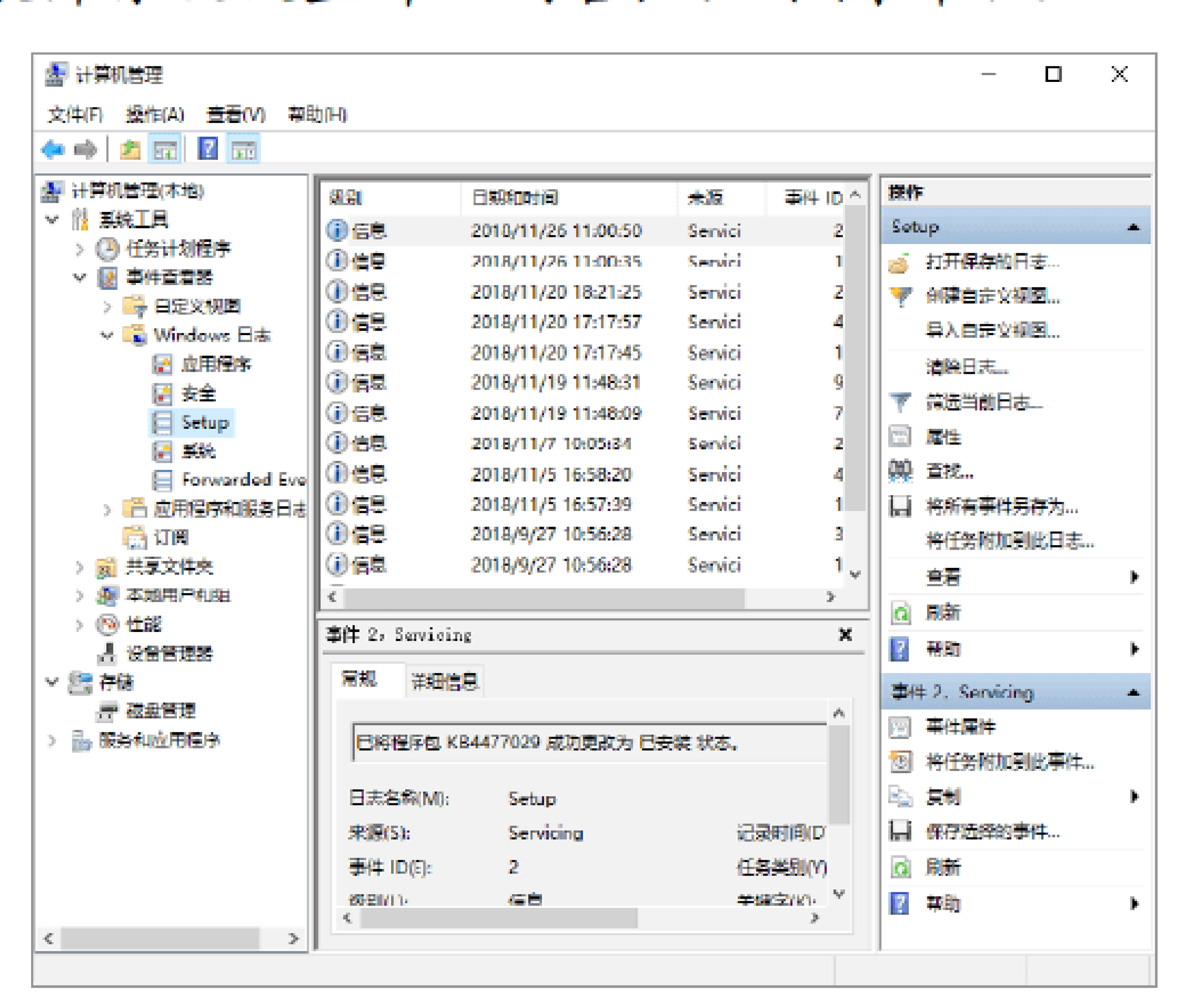
Step 09 单击“保存”按钮，即可保存事件，并弹出“显示信息”对话框，如下图所示，在其中设置是否要在其他计算机中正确查看此日志，设置完毕后，单击“确定”按钮即可保存设置。



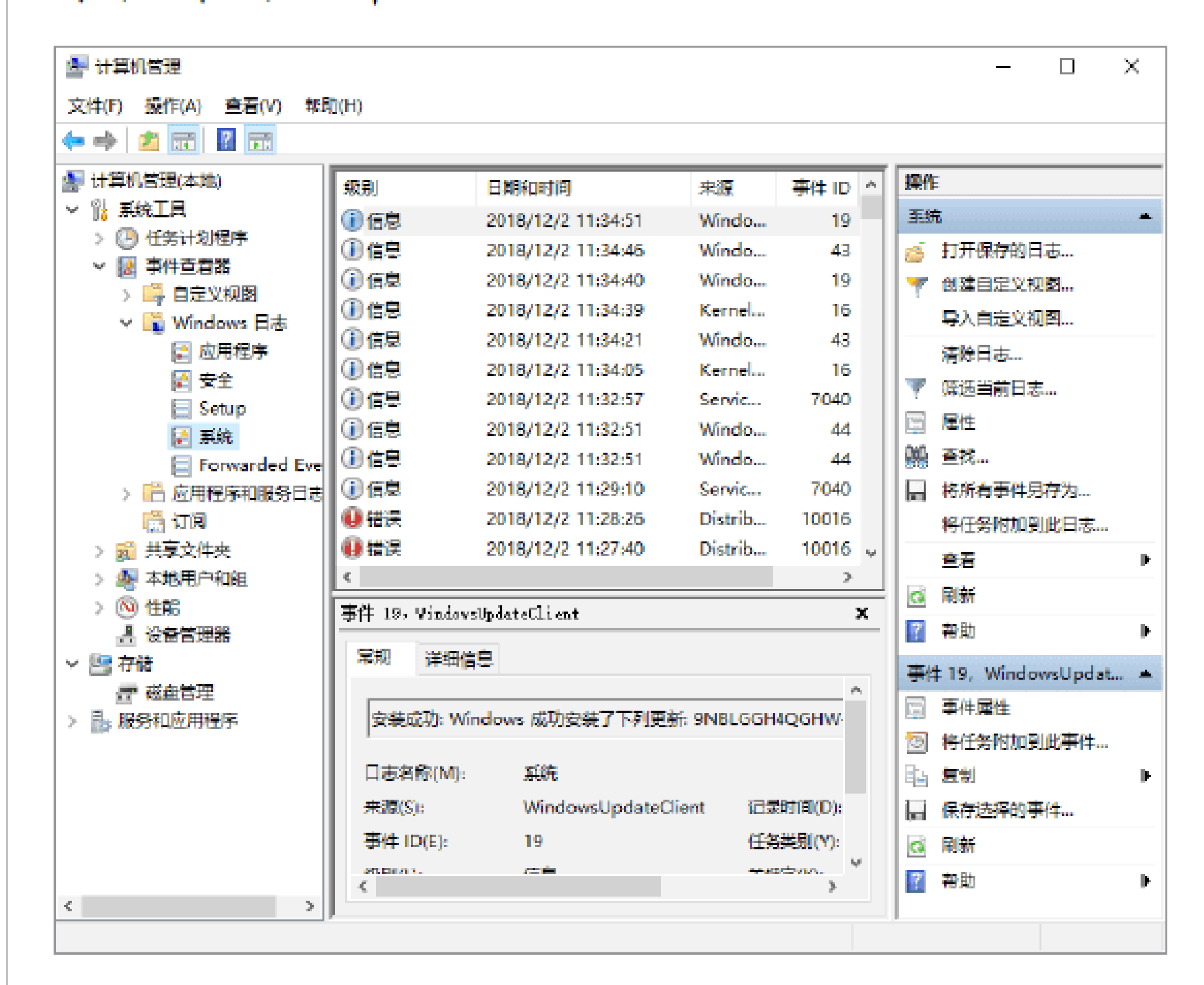
Step 10 双击左侧的“安全”选项，可以将计算机记录的安全性事件信息全都枚举于此，用户可以对其进行具体查看和保存、附加程序等，如下图所示。



Step 11 双击左侧的Setup选项，在右侧将会展开系统设置详细内容，如下图所示。



Step 12 双击左侧的“系统”选项，会在右侧看到Windows操作系统运行时内核以及上层软硬件之间的运行记录，如下图所示。这里会记录大量的错误信息，是黑客们分析目标计算机漏洞时最常用到的信息库，用户最好熟悉错误码，这样可以提高查找间谍软件的效率。

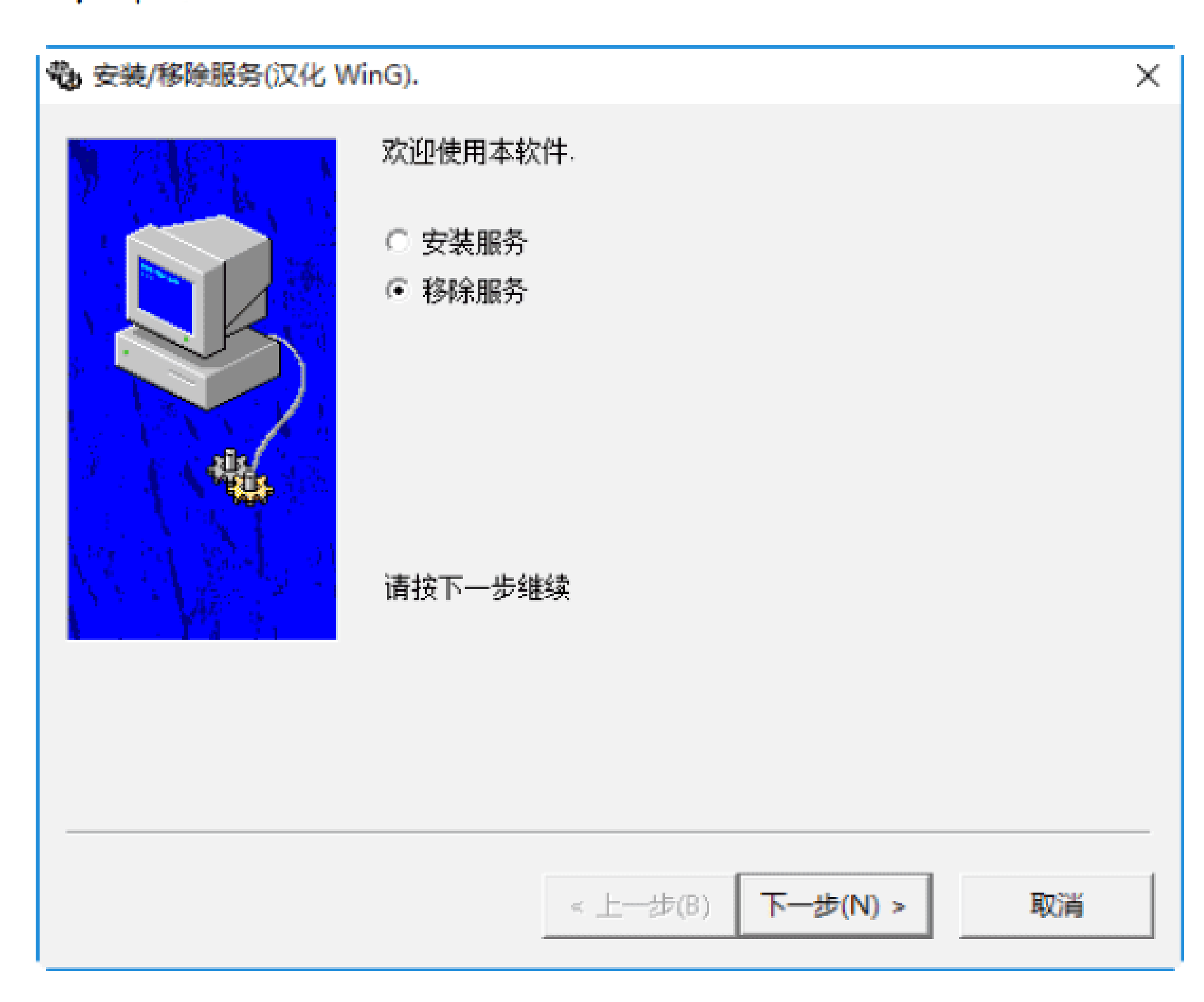


实战演练2——利用SRVINSTW删除系统服务日志



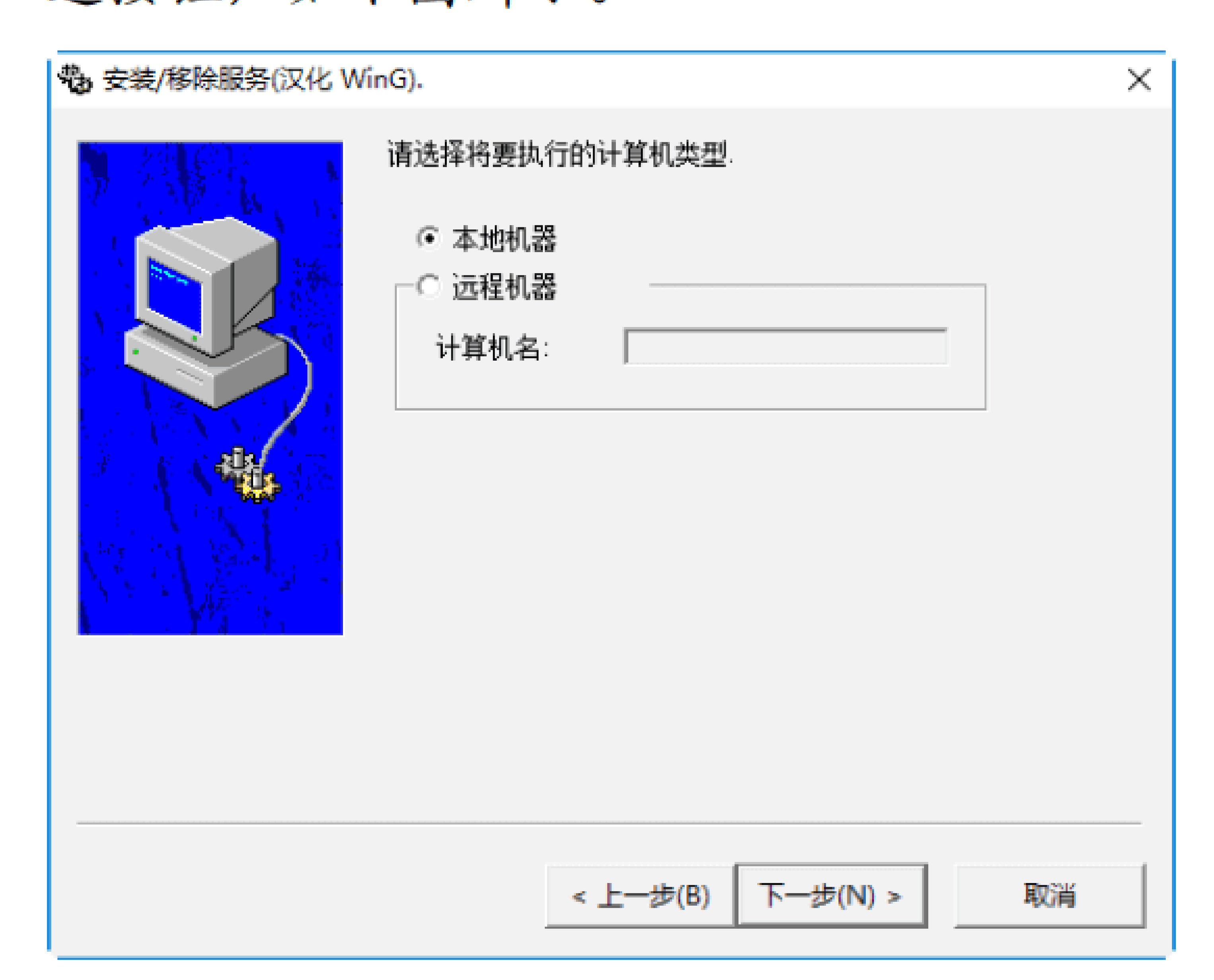
黑客可以使用SRVINSTW删除远程主机上的系统服务日志，以达到破坏的目的。删除服务日志的具体操作步骤如下。

Step 01 如果黑客已经通过图形界面控制对方的计算机，在该计算机上运行SRVINSTW.exe程序，即可打开选择操作类型对话框，在其中选中“移除服务”单选按钮，如下图所示。



Step 02 单击“下一步”按钮，即可打开计算

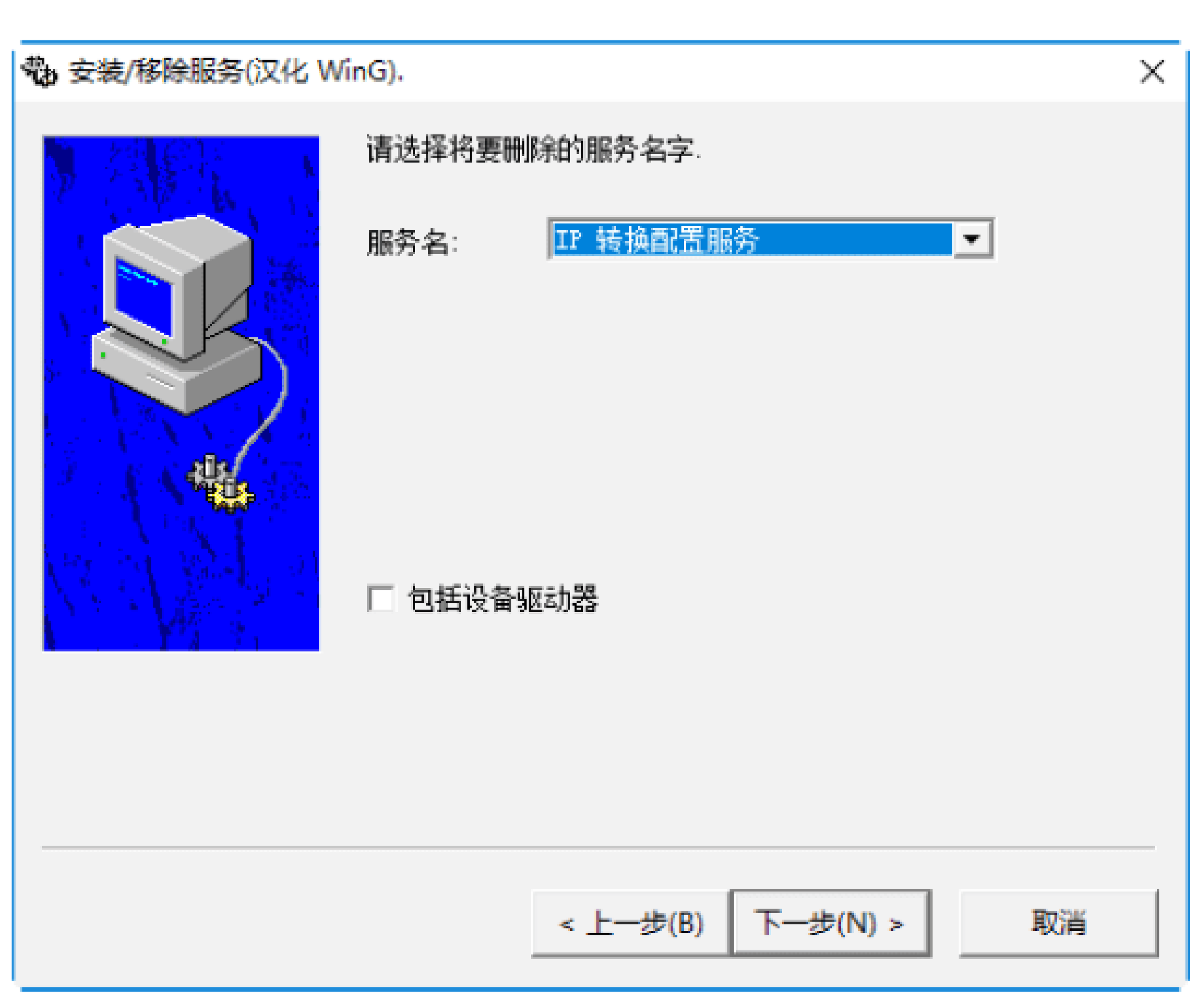
机类型选择对话框，在“请选择要执行的计算机类型”栏目中选中“本地机器”单选按钮，如下图所示。



提示：如果没有控制目标的计算机，但已经和对方建立具有管理员权限的IPC$连接，此时应该在计算机类型选择对话框中选中“远程机器”单选按钮，并在“计算机名”文本框中输入远程计算机的IP地址，单击“下一步”按钮，同样可以将该远程主机中的服务删除。



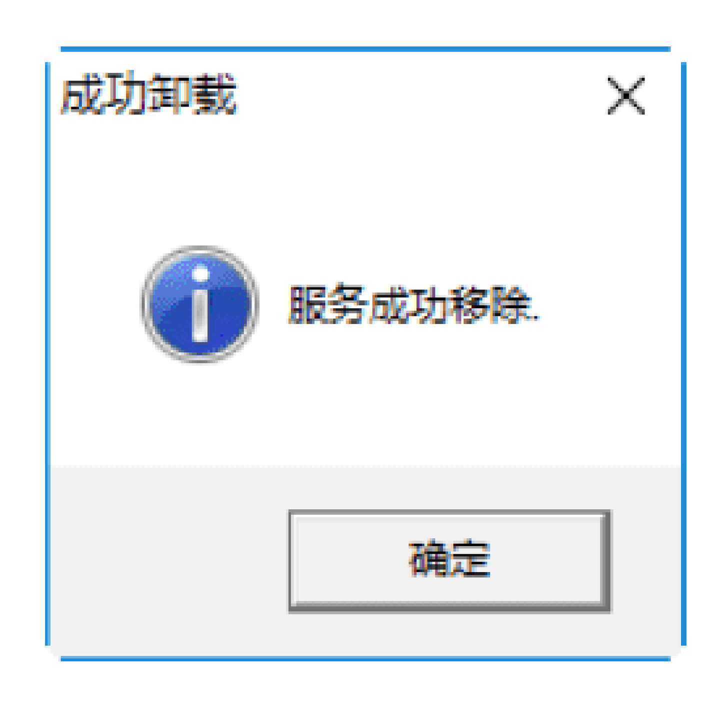
Step 03 单击“下一步”按钮，即可打开服务名选择对话框，在“服务名”下拉列表中选择需要删除的服务选项，这里选择“IP转换配置服务”选项，如下图所示。



Step 04 单击“下一步”按钮，即可打开准备好移除服务对话框，如下图所示。



Step 05 如果确定要删除该服务，单击“完成”按钮，即可看到“服务成功移除”提示框，如下图所示。单击“确定”按钮，即可将远程主机中的服务删除。



15.5 小试身手

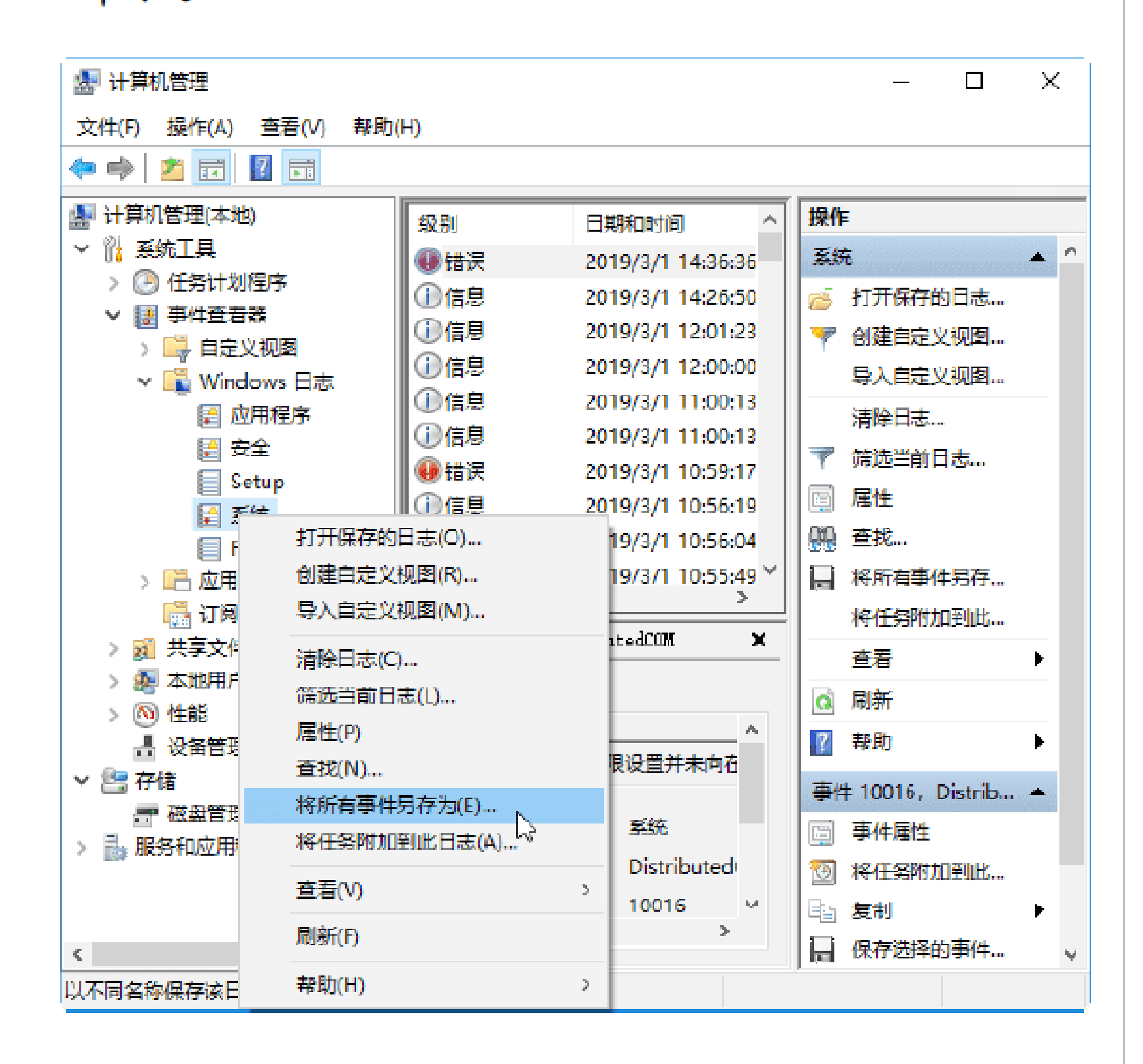
练习1：保存日志文件

将日志文件存档可以方便分析日志信息，从而找出异常日志信息，将日志文件存档的具体操作步骤如下。

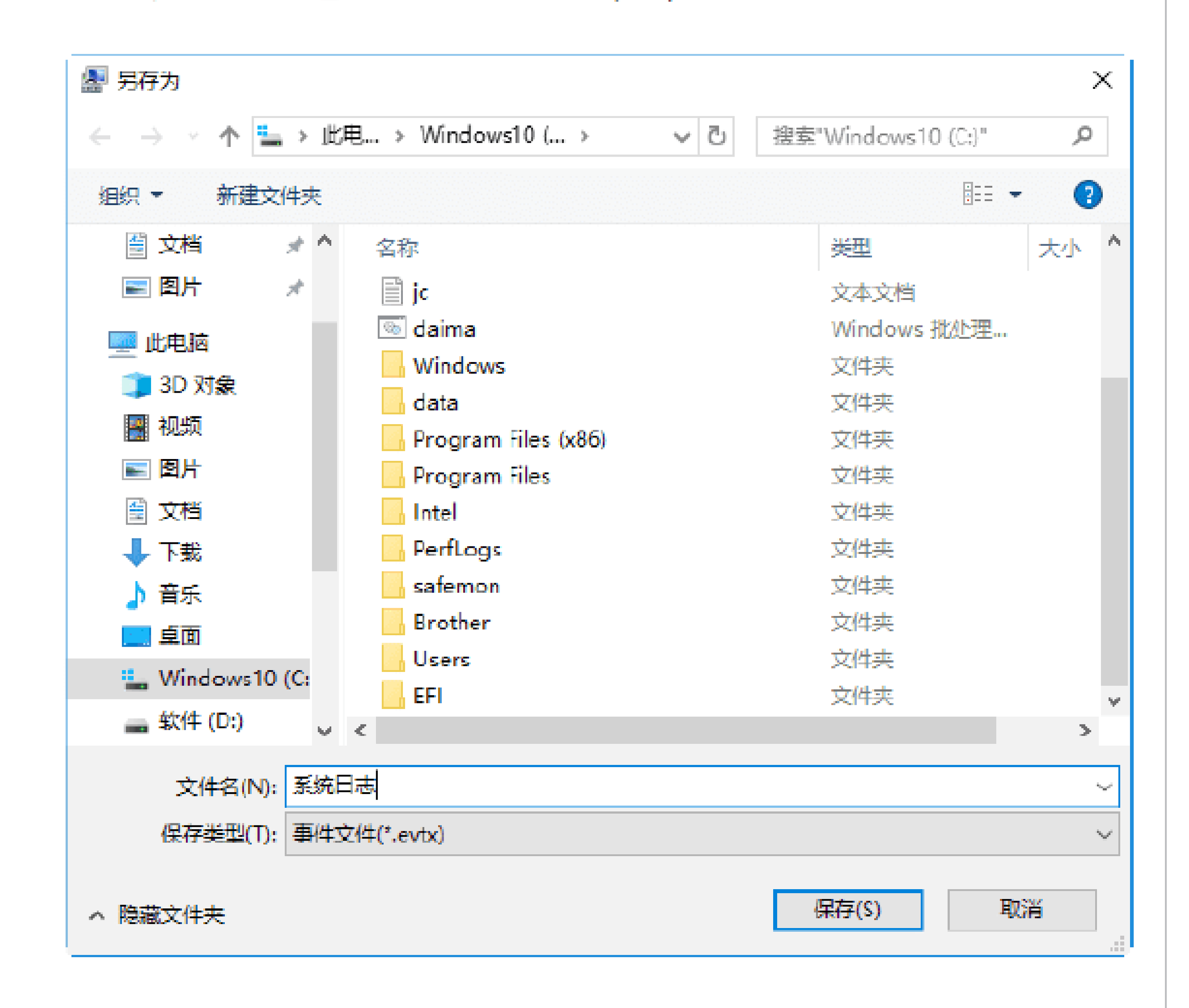
Step 01 右击“开始”按钮，在弹出的快捷菜单中选择“计算机管理”选项，如下图所示。



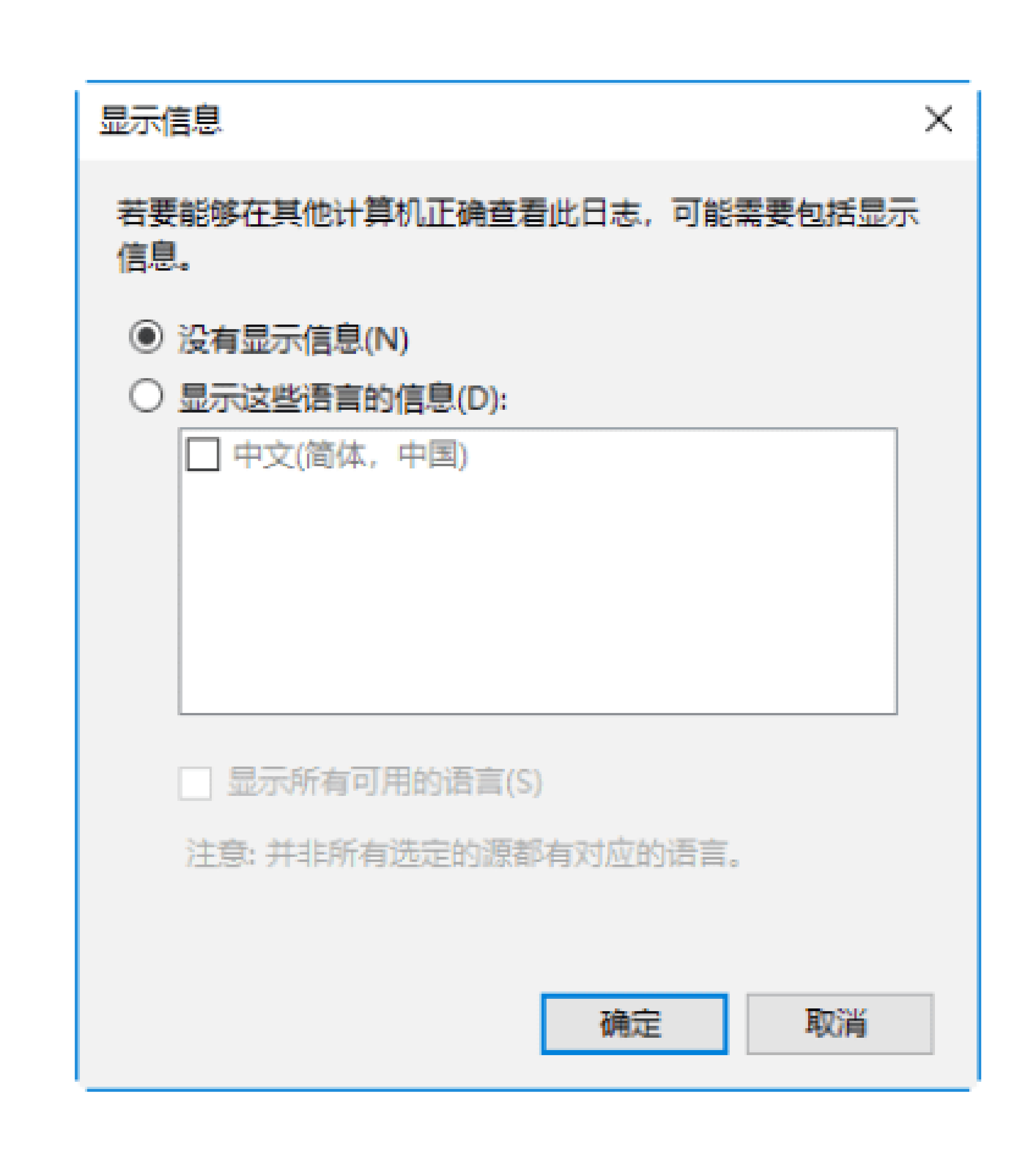
Step 02 打开“计算机管理”窗口，在其中展开“事件查看器”图标，右击要保存的日志，如这里选择“Windows日志”选项下的“系统”选项，在弹出的快捷菜单中选择“将所有事件另存为”选项，如下图所示。



Step 03 打开“另存为”对话框，在“文件名”文本框中输入日志名称，这里输入“系统日志”，如下图所示。



Step 04 单击“保存”按钮，弹出“显示信息”对话框，在其中设置相应的参数，如下图所示，然后单击“确定”按钮，即可将日志文件保存到本地计算机。



练习2：将程序固定到任务栏



在Windows 10中取消了快速启动工具栏，若要快速打开程序，可以将程序固定到任务栏，具体的方法如下。

方法1：如果程序已经打开，在“任务栏”上选择程序并右击鼠标，从弹出的快捷菜单中选择“固定到任务栏”选项，如下图所示，则任务栏上将会一直存在添加的应用程序，用户可以随时打开程序。



方法2：如果程序没有打开，选择“开始”→“所有应用”选项，在弹出的列表中选择需要添加的任务栏中的应用程序，右击鼠标并在弹出的快捷菜单中选择“固定到任务栏”选项，即可将该应用程序添加到任务栏中，如下图所示。

